2013-12

The role of state and local jurisdictions in identifying and protecting critical infrastructure

Christopoulos, Chris, Jr.

Monterey, California: Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

THE ROLE OF STATE AND LOCAL JURISDICTIONS IN IDENTIFYING AND PROTECTING CRITICAL INFRASTRUCTURE

by

Chris Christopoulos, Jr.

December 2013

Thesis Co-Advisors: Rudolf Darken
Ryan Ellis

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** December 2013	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE THE ROLE OF STATE AND LOCAL JURISDICTIONS IN IDENTIFYING AND PROTECTING CRITICAL INFRASTRUCTURE		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Chris Christopoulos, Jr.			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB protocol number ____N/A____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE** A	

13. ABSTRACT (maximum 200 words)

Over the last several years, the after effects of several major disasters have severely impacted state, local, and regional critical infrastructure. Research was conducted via an analysis of the National Infrastructure Protection program and a case study of the State of New Hampshire Critical Infrastructure Program to determine to what extent the federal criteria for identifying federal critical infrastructure and key resources apply to state and local identification of critical infrastructure and key resources. The analysis of the *National Infrastructure Protection Plan* and subsequent sector-specific plans indicates that there is no clear connection between the *National Infrastructure Protection Plan* and local government critical infrastructure and key resources protection and resiliency planning. Research also found that despite clear references to engaging state and local jurisdictions in planning, there was no evidence to support collaboration efforts between federal, state, and local jurisdictions.

14. SUBJECT TERMS critical infrastructure; state; local; National Infrastructure Protection Plan; resiliency; and collaboration			**15. NUMBER OF PAGES** 99
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

THE ROLE OF STATE AND LOCAL JURISDICTIONS IN IDENTIFYING AND PROTECTING CRITICAL INFRASTRUCTURE

Chris Christopoulos, Jr.
Fire Chief and Emergency Management Director, Lebanon Fire Department,
Lebanon, NH
B.S., Granite State College, 2010

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
December 2013

Author: Chris Christopoulos, Jr.

Approved by: Rudolf Darken
Thesis Co-Advisor

Ryan Ellis
Thesis Co-Advisor

Mohammed Hafez
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Over the last several years, the after effects of several major disasters have severely impacted state, local, and regional critical infrastructure. Research was conducted via an analysis of the National Infrastructure Protection program and a case study of the State of New Hampshire Critical Infrastructure Program to determine to what extent the federal criteria for identifying federal critical infrastructure and key resources apply to state and local identification of critical infrastructure and key resources. The analysis of the National Infrastructure Protection Plan and subsequent sector-specific plans indicates that there is no clear connection between the National Infrastructure Protection Plan and local government critical infrastructure and key resources protection and resiliency planning. Research also found that despite clear references to engaging state and local jurisdictions in planning, there was no evidence to support collaboration efforts between federal, state, and local jurisdictions.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ACEPS	Advisory Council on Preparedness and Security
CFATS	Chemical Facility Anti-Terrorism Standards
CI	critical infrastructure
CIKR	critical infrastructure and key resources
CIP	Critical Infrastructure Program
DHS	Department of Homeland Security
DIB	defense industrial base
EAS	emergency alert system
EPA	Environmental Protective Agency
ESS	emergency services sector
FAS-CAT	food and agriculture sector-criticality assessment tool
FBIIC	Federal Banking Information Infrastructure Committee
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
FOUO	for official use only
GAO	General Accounting Office
INIPP	Interim National Infrastructure Protection Program
IT	information technology
NCFPD	National Center for Food Protection and Defense
NCIPP	National Critical Infrastructure Prioritization Program
NCS	National Communications System
NRC	Nuclear Regulatory Commission
NIPP	National Infrastructure Protection Program
NPPD/IP	National Protection and Programs Directorate Office of Infrastructure Protection
NS/EP	National Security and Emergency Preparedness
PCCIP	President's Commission on Critical Infrastructure Protection
PCII	protected critical infrastructure information
PPD	presidential policy directive
PSAP	public safety answering points

RAWG	Risk Assessment Work Group
SLTTGCC	State, Local, Tribal, and Territorial Government Coordinating Council
SSA	sector specific agency
SCC	Sector Coordinating Council
SSP	sector specific plan
VIPP	Vermont Infrastructure Protection Program

EXECUTIVE SUMMARY

The terrorist attacks of September 11, 2001, Hurricane Katrina in 2005, "Super Storm" Sandy in 2012, and the recent widespread flooding in Colorado and associated damages to critical infrastructure, only reinforce the need for collaboration between federal, state, and local government for pre-event planning, preparation, response, and recovery.

Research conducted sought to examine the relationship between the National Infrastructure Protection Program and state and local critical infrastructure planning. Specifically, to what extent does the federal criteria for identifying federal critical infrastructure and key resources apply to state and local identification of critical infrastructure and key resources (CIKR). As the first line of defense and response to incidents within their jurisdictions, local officials must work to identify what critical infrastructure exists within and more importantly, if lost, what will have an impact on the community's ability to provide services.

Research included a comprehensive analysis of the *National Infrastructure Protection Plan* (NIPP) and all open source critical infrastructure sector-specific plans. A case study of the state of New Hampshire Critical Infrastructure Program was also included as an example of a "model program" for state governments.

The analysis of the NIPP and subsequent sector-specific plans indicates that there is no clear connection between the NIPP and local government CIKR protection and resiliency planning. Research also concluded that, while some states have worked to develop CIKR plans, and do participate in the Annual Federal Data Call or the National Critical Infrastructure Prioritization Program, it is unclear on the extent of participation or the number of assets reported. Conversely, all 50 states and approximately 70 percent of the communities in the U.S. have approved hazard mitigation plans under the Federal Emergency Management Agency's Pre-Disaster Mitigation Program since its inception.[1] Between 2007 and 2012, FEMA awarded $1.7 billion in Hazard Mitigation Planning

[1] Office of the Inspector General, U.S. Department of Homeland Security, *Survey of Hazard Mitigation Planning*, 2012, http://www.oig.dhs.gov/assets/Mgmt/2012/OIG_12-109_Aug12.pdf, 1.

Grants.[2] During a similar period FEMA spent over $17.3 billion on disaster relief.[3] This data suggests that the U.S. is not committing sufficient resources towards prevention and mitigation of the impacts associated with natural and manmade disasters and that inaction related to CI protection and more importantly, resiliency planning is more costly.

This thesis suggests three major recommendations for better alignment of federal, state, and local critical infrastructure planning.

- Strengthen the relationship between federal, state, and local critical infrastructure planning. This can be accomplished by 1) Redefining the CIKR reporting process from a "top down" to an "up and down" information flow and 2) Implementing the goals and objectives related to information sharing at the state and local Levels as identified in the *National Strategy for Information Sharing and Safeguarding*.[4]
- Link hazard mitigation planning with national infrastructure protection and resiliency planning. Each planning process focuses on a risk assessment strategy for assessing and identifying critical assets, networks, and systems. This recommendation suggests the development of a "hybrid" planning process incorporating key elements of hazard mitigation planning and the NIPP.
- Create standard asset definitions for all CIKR sectors. Creating a standard, scalable consequence based criteria will provide clear guidance for developing CIKR lists at the federal, state and local Level. Consequence definitions will allow planner at all Levels to assess assets, systems, and networks in a uniform manner and in most cases are easier to identify.

[2] Office of the Inspector General, U.S. Department of Homeland Security, *Survey of Hazard Mitigation Planning*, 2012, http://www.oig.dhs.gov/assets/Mgmt/2012/OIG_12-109_Aug12.pdf.

[3] Office of Budget and Management, *OMB Report on Disaster Relief Funding to the Committees on Appropriations and the Budget of the U.S. House of Representatives and the Senate*, 2011. http://www.whitehouse.gov/sites/default/files/omb/assets/legislative_reports/disaster_relief_report_sept2011.pdf.

[4] White House, *National Strategy for Information Sharing and Safeguarding*, 2012, http://www.whitehouse.gov/sites/default/files/docs/2012sharingstrategy_1.pdf.

ACKNOWLEDGMENTS

I feel very blessed with the opportunity to participate in the Naval Postgraduate School, Center for Homeland Defense and Security, master's program. I have shared many great life and learning experiences with new lifelong friends. This thesis would not have been possible without the guidance and occasional kick in the rear of Christopher Pope, State of New Hampshire Homeland Security Director (retired). Professors Rudy Darken and Ryan Ellis, you helped me turn an idea into a thesis that will hopefully help to protect the health and safety of local communities.

Foremost, I thank my wife and best friend (and initial editor for all course work) Lori, without your love and support I would have never made it through this experience and I will cherish you always! To my stepsons, JT and Nick and stepdaughter, Justina—I am sorry for missing important school or sporting events, but thank you for your support and for helping deal with household chores, etc.

I am thankful to the men and women of the Lebanon Fire Department for your professionalism and carrying forward the mission of the organization in my absences over the past two years. Thank you to Lebanon City Manager Greg Lewis for your support of my attending this program and my overall professional development. Chief Jack McElfish, Sandy Springs Fire Department, GA; Chief William S. "Wiggy" Johnson, Jr. (retired), West Haven Fire Department, CT; and Captain Michal Callan (retired), Wallingford Fire Department, CT—each of you has made me a better firefighter, leader, and person in your own unique way and I thank you!

Lastly, I dedicate this thesis to my father, Connecticut State Trooper 1st Class Chris Christopoulos, Sr., who passed over 13 years ago. I know you are here with me in spirit, and I thank you for showing me the pathway to public service.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

"Emergency Preparedness is a Team Sport"[1]

A. PROBLEM STATEMENT

Most recently, *Presidential Policy Directive 21* (PPD-21), signed by President Obama on February 12, 2013, redefined the federal approach from the current *Critical Infrastructure Protection to Critical Infrastructure Security and Resilience*.[2] PPD-21 states the following among three strategic imperatives:

> Refine and Clarify Functional Relationships across the Federal Government to Advance the National Unity of Effort to Strengthen Critical Infrastructure Security and Resilience
>
> An effective national effort to strengthen critical infrastructure security and resilience must be guided by a national plan that identifies roles and responsibilities and is informed by the expertise, experience, capabilities, and responsibilities of the SSAs, other Federal departments and agencies with critical infrastructure roles, State, local, tribal and territorial entities, and critical infrastructure owners and operators.[3]

Federal critical infrastructure protection programs pre-date PPD-21, including the *National Infrastructure Protection Plan* (NIPP). It was in 2008 to address the national policy for critical infrastructure protection and key resource (CIKR) protection requirements set forth in *Presidential Decision Directive 7: Critical Infrastructure (CI) Identification, Prioritization, and Protection* (PDD-7).[4] The primary goal of the NIPP is to:

---

[1] Eric Whitaker, "Preparing for a Disaster," Dictionary Quotes, July 2012, http://www.dictionary-quotes.com/emergency-preparedness-is-a-team-sport-eric-whitaker/.

[2] White House, *Presidential Policy Directive 21: Critical Infrastructure Security and* Resiliency, 2013, White House, http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[3] Ibid.

[4] White House, *Presidential Decision Directive 7: Critical Infrastructure Identification, Prioritization, and Protection*, 2003, Department of Homeland Security, http://www.dhs.gov/homeland-security-presidential-directive-7.

> …build a safer, more secure, and more resilient America by preventing, deterring, neutralizing, or mitigating the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit elements of our nation's CIKR and to strengthen national preparedness, timely response and rapid recovery of CIKR in the event of an attack, natural disaster, or other emergency."[5]

Recognizing that certain federal, state, and local assets can be critical to the continuity of government operations, the NIPP provides the framework for developing critical infrastructure protection programs for all Levels of government.

The NIPP also states, but does not mandate, that "State and local governments are responsible for implementing the homeland security mission, protecting public safety and welfare, and ensuring the provision of essential services to communities and industries within their jurisdictions."[6] This suggests that state and local jurisdictions are a major stakeholder role in the protection of CI and the development of asset lists.

This thesis will analyze the relationship between the federal NIPP and local jurisdictions, the federal methodology for defining CI, and the importance of integrating local officials in the development of critical infrastructure protection planning. Specifically, research will seek to determine how or if the federal criteria for determining CIKR assets can assist state and local governments in developing CIKR protection and resiliency plans and why this might be important. Conversely, what role do state and local CIKR protection plans play within the federal NIPP?

Over the last several years the United States has experienced natural and manmade disasters that have severely impacted critical infrastructure. For example, in 2005 Hurricane Katrina struck the United States Gulf Coast, virtually "collapsing all critical infrastructures at the same time."[7] The *White House Katrina Report* described the loss of one sector, the communications infrastructure as follows, "The complete devastation of this infrastructure left first responders without a reliable network to use for

---

[5] U.S. Department of Homeland Security, *National Infrastructure Protection Plan*, 2009, Department of Homeland Security, http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

[6] Ibid., 21.

[7] Robert Miller, "Hurricane Katrina: Communications & Infrastructure Impacts," in *Threats at Our Threshold*, 2012, http://astrumsat.com/wp-content/uploads/2012/04/KatrinaHurricaneComm.pdf.

coordinating emergency response."[8] The Katrina report also found that "Federal, state and local officials responded to Hurricane Katrina without comprehensive understanding of the interdependencies of the Critical Infrastructure sectors in each geographical area and the potential national impact of their decisions."[9]

The report further states:

> Federal, State, and local officials need an implementation plan for critical infrastructure and restoration that can be shared across the Federal government, State and local governments, and with the private sector, to provide them with the necessary background to make informed preparedness decisions with limited resources."[10]

Seven years later, Super Storm Sandy caused major damage to utility, transportation systems, health care facilities, water and waste water treatment facilities and communications systems throughout the Atlantic coastal region. Damages estimates are in the billions of dollars.[11] The Hurricane Sandy Rebuilding Task Force lists extensive recommendations related to infrastructure resiliency and simply states "examples from Sandy that illustrate the need for regional coordination of resilience investments were seen in many instances."[12] One recurring theme amongst the references is the need to engage state and local jurisdictions in the identification and protection of critical infrastructure assets. The incidents cited highlight the failures, despite the numerous references to the important role of state and local jurisdictions, of proactive CIKR planning at all Levels of government. Whether or not the goal of CI programs is protection (PPD-7) or security and resilience (PPD-21), the importance of

---

[8] White House, "The Federal Response to Hurricane Katrina: Lessons Learned," 2006, White House Archives, http://georgewbush-whitehouse.archives.gov/reports/katrina-lessons-learned/chapter5.html.

[9] Ibid., 61.

[10] Ibid.

[11] Hurricane Sandy Rebuilding Task Force, "Fact Sheet: Progress to Date," August 19, 2013, U.S. Department of Housing and Urban Development, http://portal.hud.gov/hudportal/HUD?src=/press/press_releases_media_advisories/2013/HUDNo.13-125, 24.

[12] Ibid., 54.

communicating with, and including state and local jurisdictions cannot be minimized. Each example above stresses the importance for state and local jurisdictions to understand, assess and identify of CI assets.

While CI assets affected by any of the above incidents might not have been specifically protected or meet the criteria for protection, it begs to question the effectiveness or applicability of the NIPP for state, local, tribal, and territorial governments. The Katrina report references the interim NIPP as "providing strategic-Level guidance for Federal, State and local entities to use in prioritizing infrastructure for protection."[13] However, literature does not outline a plan for implementing plans.

The introduction of the NIPP states, "Protecting and ensuring the continuity of the Critical Infrastructure and Key Resources (CIKR) of the United States is essential to the Nation's security, public health and safety, economic vitality, and way of life."[14] With emphasis on the word essential, it becomes clear that CI protection and resiliency planning must be implemented at the state and local Level, and not just a federal effort. Lastly, creating standard definitions for identifying CI assets, systems, and networks will allow state and local governments to develop CI protection and resiliency plans that augment federal plans.

B. RESEARCH QUESTIONS

- To what extent could the federal criteria for identifying federal critical infrastructure and key resources apply to state and local identification of critical infrastructure and key resources?
- Should critical infrastructure protection and resiliency planning be important to state and local governments?

C. ARGUMENT

Every community in this country has some asset(s), which, in the event of failure, would have a significant impact on the community or region. Assets could simply be a roadway, community well, reservoir, culvert pipe, or health care facility or a complex

[13] White House, "The Federal Response to Hurricane Katrina," 61.

[14] U.S. Department of Homeland Security, *National Infrastructure Protection Plan*, 1.

system, such as a water or waste water treatment facility. In *Critical Infrastructure Protection in Homeland Security*, Ted Lewis claims, "Critical infrastructure protection is too big for state and local governments to handle on their own" and "infrastructures are, for the most part, national assets."[15] While this may be true for sectors, such as telecommunications, energy (oil, pipeline, electricity) and some transportation assets, other sectors, such as potable water treatment and delivery, waste water treatment, or health care are located in and the responsibility for primary emergency response often lies with local jurisdictions.

D. SIGNIFICANCE OF THE RESEARCH

This research will propose to identify the importance of engaging local jurisdictions in the development of local definitions for CIKR assets. The merits of this effort and possible outcomes will be development of a CIKR flow model that interconnects federal, state and local definitions. This information would allow local governments to develop CIKR protection strategies, develop resiliency plans, better mitigate natural and manmade disasters and develop partnerships with the private sector. Furthermore, the development of state and local definitions for CIKR assets will better assist jurisdictions with indentifying CIKR and developing CIKR protection and resiliency plans.

E. CHAPTER OVERVIEW

The focus of this thesis centers on the applicability of the National Infrastructure Protection Program to local jurisdictions. Chapter II provides a summary of relevant literature and identifies the lack of available resources related to local critical infrastructure plans. Chapter III will frame the research methodology and limitations used to answer the research question. Chapter IV provides an overview and comparison of the current NIPP and the expected changes in the NIPP as a result of PPD-21. This chapter also lays out one approach to critical infrastructure protection planning through a case study on the state of New Hampshire Critical Infrastructure Protection Program.

[15] Ted G. Lewis, *Critical Infrastructure Protection in Homeland Security* (Hoboken, NJ: John Wiley & Sons, 2006), 10.

Chapter V will summarize the key findings and offer recommendations for improving critical infrastructure protection and resiliency programs for local jurisdictions. Lastly, Chapter VI will present some final thoughts on critical infrastructure protection and resiliency and suggest future research topics.

F. CONCLUSION

No matter who owns critical infrastructure assets, private companies, federal, state or local governments, most of these assets will have some contact with local jurisdictions. History has proven that many local jurisdictions are ill prepared to respond to, protect or assist in the recovery of these key assets and therefore must be engaged in the development of CIKR asset lists at all Levels of government. Furthermore, CI protection and resiliency planning must include an "all-hazards" approach. Of the 787 major disaster declarations for the years 2001–2013, only two can be attributed to terrorism.[16] Without diminishing the effects of a terrorist event, this statistic suggests that communities are much more likely to experience a natural disaster over a terrorist attack.

[16] Federal Emergency Management Agency, "Disaster Declarations," Federal Emergency Management Agency, accessed August14, 2013, http://www.fema.gov/disasters/grid/year.

II. LITERATURE REVIEW

According to the 2003 *State Officials Guide to Critical Infrastructure Protection* (CIP), there are 75,000+ state and locally owned dams and reservoirs, 700,000+ miles of drinking water networks, 5,800+ hospitals, over 87,000 emergency service/law enforcement agencies, 104 commercial nuclear power plants, 100,000+ miles of railroad and 5,000+ public airports and many other identified critical infrastructure located throughout the United States.[17] While the federal government has an interest in protecting CI of national significance, most of the CI above is located in local jurisdictions. This places tremendous responsibility for protecting CI assets on state and local jurisdictions.

The materials reviewed include: government reports, federal infrastructure protection guidance documents, state homeland security strategies, federal hazard mitigation planning guides and foundation reports.

A. WHAT IS CRITICAL INFRASTRUCTURE?

While infrastructures have always been important at the federal, state, and local Levels, critical infrastructure identification dates back several hundred years with the development of systems, such as the postal service that "sustain our way of life."[18] However, formal definitions were not developed until the late 1990s In May 1998, President Clinton issued *Presidential Decision Directive/NSC 63* (PPD-63), which defines CI as, "those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private."[19] This directive identified a total

[17] Council of State Governments, "State Officials Guide to Critical Infrastructure," 2003, Council of State Governments http://www.csg.org/knowledgecenter/docs/SOG03CriticalInfrastructure.pdf.

[18] Ibid. p.4

[19] White House, *Presidential Decision Directive/NSC 63*, 1998, Federation of American Scientists, http://www.fas.org/irp/offdocs/pdd/pdd-63.htm.

of 10 specific sectors with liaisons and four special topic areas.[20] The directives outlined in PPD-63 were a result of the recommendations by the President's Commission on Critical Infrastructure Protection (PCCIP). The PPCIP was established in 1996 was tasked with reporting to the president on the threats and vulnerabilities to the nation's critical infrastructure.[21]

The Department of Homeland Security has adopted the definition from the U.S. PATRIOT Act, which defines CI as "the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof."[22] This definition amended to include intentional acts as a result of the terrorist attacks of September 11, 2001. While the definitions in PPD-63 and the PATRIOT Act are very similar, the definition provided in *Presidential Decision Directive/NSC 63* was developed in the "structure for implementing CI policy and a limited scope in the specific sectors."[23] The United States PATRIOT Act definition provides for a broader spectrum of CI assets and threats and led to the expansion of the CI sectors to 18.

B. FEDERAL GUIDANCE

In 2005, the United States Department of Homeland Security released the *Interim National Infrastructure Protection Plan* (INIPP) as a "starting point for developing the national, cross-sector plan for Critical Infrastructure Protection."[24] This plan identified 17 CI asset sectors and assigned each sector to a "sector specific" agency. Sector specific agencies are responsible for identifying sectors assets, systems, and networks,

---

[20] Ibid.

[21] President's Commission on Critical Infrastructure Protection, "Critical Foundations—Protecting America's Infrastructure," 1997, Federation of American Scientists, http://www.fas.org/sgp/library/pccip.pdf.

[22] Department of Homeland Security, "Critical Infrastructure Protection," Department of Homeland Security, http://www.dhs.gov/critical-infrastructure.

[23] Council of State Governments, "State Officials Guide to Critical Infrastructure," 5.

[24] U.S. Department of Homeland Security, *Interim National Infrastructure Protection Plan*, 2005, Educase, http://net.educause.edu/ir/library/pdf/csd3754.pdf.

interdependencies, and for establishing risk assessment guidelines for the sector. Furthermore, this plan listed the following as key stakeholders and partnerships: Department of Homeland Security; sector-specific agencies; private sector; and state, local, and tribal entities.[25] Goal 4 of the INIPP states, "Build Partnerships among Federal, State, local, tribal, international, and private sector stakeholders to implement Critical Infrastructure Protection Programs."[26] This would suggest that collaborative approach is needed to develop effective CIKR protection plans.

The *National Infrastructure Protection Plan* was released in 2008 to address the national policy for critical infrastructure protection and key resource protection (CIKR) requirements set forth in *Presidential Decision Directive 7: Critical Infrastructure Identification, Prioritization, and Protection* (PDD-7).[27] The NIPP emphasizes the inclusion of key partners, such as state, local, tribal and territorial governments for the implementation.[28] The theme of specifically including state and local governments pre-dates the Interim NIPP and the 2008 NIPP. The earliest reference found in *GAO-01-323, Critical Infrastructure Protection* states:

> The January 2000 *National Plan for Information Systems Protection*, the role of the federal government is to encourage nonfederal entities (the private sector and state and local governments) to organize themselves for efficient information exchange about cyber threats and incidents.[29]

State and local jurisdictions are identified as "key stakeholders" in the effort to protecting Critical Infrastructure and sharing information related to threats, vulnerabilities, and consequences associated with failure of CI.

Furthermore, the NIPP and PDD-7 identifies 18 sectors for CIKR and assigns each a "sector-specific agency" that is responsible for developing federal CIKR sector

---

[25] Ibid. p.4

[26] Ibid., 8

[27] White House, *Presidential Decision Directive 7*.

[28] U.S. Department of Homeland Security, *National Infrastructure Protection Plan*, 2.

[29] General Accounting Office, *Critical Infrastructure Protection* (GAO-01-323), 2001, Homeland Security Digital Library, https://www.hsdl.org/?view&did=197.

specific criteria.[30] For example, the water sector has been assigned to the Environmental Protection Agency (EPA).[31] EPA has established the criteria for determining nationally significant assets in the water sector in a sector-specific plan.[32] Each sector-specific agency is then responsible for developing criteria for defining CI within the sector. For example, in order to meet the federal tier Levels, critical water treatment facilities are assessed based on: 1) population served; 2) on-site gaseous chlorine storage; 3) Economic loss impact; and 4) critical customers served.[33]

The benefits of implementing the NIPP are listed as:[34]

- Understanding of CIKR assets, systems, networks, and facilities, and other capabilities through industry ownership and management of a vast majority of CIKR in most sectors;
- Ability to take action to reduce risk and to respond to and recover from incidents;
- Ability to innovate and to provide products, services, and technologies to quickly focus on mission needs; and
- Robust relationships that are useful for sharing and protecting sensitive information regarding threats, vulnerabilities, countermeasures, and best practices.

Despite numerous references to state and local partners and stated benefits, clear guidance for defining critical assets, networks, and systems for State and local jurisdictions is absent.

C. STATE STRATEGIES FOR CIKR PROTECTION

A limited review of readily available state homeland security strategies and state critical infrastructure protection programs for New Hampshire, Vermont, Massachusetts, Kansas, New Mexico, Missouri, Virginia, and Pennsylvania demonstrates that

---

[30] U.S. Department of Homeland Security, *National Infrastructure Protection Plan*, 1.

[31] Ibid.

[32] U.S. Environmental Protection Agency, *Water Sector-Specific Plan*, 2010, U.S. Department of Homeland Security, http://www.dhs.gov/xlibrary/assets/nipp-ssp-water-2010.pdf.

[33] Brandon Wales, *2009 Tier I and II Data Call* (Washington, DC: U.S. Department of Homeland Security, 2009) (Restricted document).

[34] U.S. Department of Homeland Security, *National Infrastructure Protection Plan*, 10.

establishing and/or classifying CI at the state Level is a priority.[35] The focus and scope of the plans vary. For example, Virginia's program mirrors the federal plan by assigning sector-specific agencies who are charged with developing state criteria.[36] New Mexico places a large emphasis on public-private collaboration but does not develop sector definitions. Furthermore, New Mexico suggests that the federal strategy promotes "stove-piping" and may limit vital communications amongst the sectors.[37] In addition, Massachusetts strategy lists a goal of "creating a common operating picture among homeland security and public safety stakeholders."[38] The objective related to CI is the "Commonwealth must be committed to providing a statewide coordinated approach to the identification, prioritization and protection of critical infrastructure and key resources and that information must be shared with important stakeholders and emergency response personnel."[39]

Another plan, the state of Vermont homeland security strategy, establishes one goal "Sustain the NIPP in Vermont" and one objective, "Implement the Vermont

---

[35] Kansas Division of Emergency Management, "Kansas State Homeland Security Strategy Goals and Objectives," 2009, http://www.accesskansas.org/kdem/EMSWeb/pdf/library/State%20Strategy%20Fall%202009%20FINAL_1.pdf; D. J. O'Neil, "Statewide Critical Infrastructure Protection: New Mexico's Model," *TR News*, no. 211 (2000); http://onlinepubs.trb.org/onlinepubs/trnews/trnews211.pdf; Office of the Inspector General, U.S. Department of Homeland Security, *State of Missouri's Management of State Homeland Security Program and Urban Areas Security Initiative Grants Awarded during Fiscal Years 2005 through 2007*, 2010, Office of the Inspector General, http://www.oig.dhs.gov/assets/Mgmt/OIG_10-33_Jan10.pdf; State of New Hampshire, Department of Safety, *State of New Hampshire Homeland Security CI/KR Identification Report*, March 10, 2008, (For official use only); E. V. Jones, V. J. Lyford, M. K. Qazi, N. J. Solan, Y. Y. Haimes, *Virginia's Critical Infrastructure Protection Study*, 2003, http://ieeexplore.ieee.org/xpl/abstractAuthors.jsp?tp=&arnumber=1242416&url=http%3A%2F%2Fieeexplore.ieee.org%2Fiel5%2F8798%2F27841%2F01242416; Office of the Inspector General, U.S. Department of Homeland Security, *Commonwealth of Pennsylvania's Management of State Homeland Security Program and Urban Areas Security Initiative Grants*, 2011, http://www.oig.dhs.gov/assets/Mgmt/OIG_11-109_Sep11.pdf; Commonwealth of Massachusetts, Executive Office of Public Safety and Security, *Commonwealth of Massachusetts Homeland Security Strategy*, 2007, http://www.mass.gov/eopss/docs/helpus-helpyou/state-homeland-security-strategy-092307.pdf; State of Vermont Division of Emergency Management and Homeland Security, *Vermont Homeland Security Strategy*, 2012, http://hsu.vermont.gov/sites/vhs/files/2013%20Vermont%20State%20Strategy%20FINAL%20101512.pdf.

[36] E. V. Jones et al., *Virginia's Critical Infrastructure Protection Study* (2003).

[37] O'Neil, *Statewide Critical Infrastructure Protection*.

[38] Commonwealth of Massachusetts, Executive Office of Public Safety and Security, *Commonwealth of Massachusetts Homeland Security Strategy*, 6.

[39] Ibid., 12.

Infrastructure Protection Plan (VIPP)" related to CI protection.[40] The scope of the VIPP is to "employ an all-hazards approach to identify and protect CIKR with statewide, regional or national implications that if lost or disrupted would have a significant detrimental impact."[41] Vermont's infrastructure plan mirrors the NIPP by assigning sector specific agencies for 18 sectors. The plan defines the scope of each sector and identifies some assets deemed critical.[42] Finally, New Hampshire does follow the federal strategy by assigning sector-specific agencies, but it limits the possibility of "stove-piping" by having all sectors report back to a main CI committee. Additionally, New Hampshire has further developed definitions for identifying CI assets that are critical to the state or region.[43] This can assist the state in developing CI protection plans and allocating grant monies for buying down risk.

D. LOCAL CIKR DEFINITIONS

While much of the literature reviewed acknowledges that most CI is located in local jurisdictions and stresses the importance of engaging local authorities, there is little information on the processes and/or suggested criteria for developing local CIKR definitions or asset lists. A 2008 DHS guide for CIKR suggests that "states, regions and communities may contain CIKR that are very important to the local economy and the safety and confidence of the population, even if they are not nationally significant."[44] Much of the literature reviewed suggests that states are encouraged to work with local jurisdictions to develop CIKR protection plans. With this said the membership of the State, Local, Tribal and Territorial Government Coordinating Council (SLTTGCC),

---

[40] State of Vermont Division of Emergency Management and Homeland Security, *Vermont Homeland Security*.

[41] State of Vermont Division of Emergency Management and Homeland Security, *Vermont Infrastructure Protection Plan*, 2009, http://vem.vermont.gov/local_state_plans/eop.

[42] Ibid., 32–42.

[43] State of New Hampshire, Department of Safety, *State of New Hampshire Homeland Security CI/KR Identification Report*.

[44] U.S. Department of Homeland Security, *A Guide to Critical Infrastructure and Key Resources Protection at the State, Regional, Local, Tribal and Territorial Level*, 2008, U.S. Department of Homeland Security, http://www.dhs.gov/xlibrary/assets/nipp_srtltt_guide.pdf.

established in 2007 in the implementation of the *National Infrastructure Protection Plan*, includes only six local cities or towns as of August 2011.[45]

Natural hazard mitigation planning, which is mandatory for state and local governments to be eligible for receiving non-emergency disaster assistance, is one process that may be looking at CIKR assets but in the context of natural disasters and not terrorism. Natural hazard mitigation planning is "the process of figuring out how to reduce or eliminate the loss of life and property damage resulting from natural hazards."[46] While this type of planning does not meet the individual sector designations found in federal and state guidance or specifically address "human caused" disasters, this process does categorize "critical buildings and facilities" in five areas: 1) essential facilities; 2) transportation systems; 3) life-line utility systems; 4) high potential loss facilities; and 5) hazardous materials facilities. While these plans only address protection from natural hazards, leveraging the process and definitions may assist local jurisdictions in developing CI protection and resiliency plans. The Federal Emergency Management Agency (FEMA) suggests there are numerous benefits to hazard mitigation planning:[47]

- Identifying cost effective actions for risk reduction that are agreed upon by stakeholders and the public;
- Focusing resources on the greatest risks and vulnerabilities;
- Building partnerships by involving people, organizations, and businesses;
- Increasing education and awareness of hazards and risk;
- Communicating priorities to state and federal officials;
- Aligning risk reduction with other community objectives.

Communities participating in hazard mitigation planning are in fact determining what assets, systems, and networks are critical to the continuity of local government

---

[45] State, Local, Tribal and Territorial Government Coordinating Council, "SLTTGCC Fact Sheet," 2011, U.S. Department of Homeland Security, http://www.dhs.gov/xlibrary/assets/slttgcc-factsheet-508-2011-08-19.pdf.

[46] Federal Emergency Management Agency, *State and Local Hazard Mitigation Planning—How-to Guide*, 2001, Federal Emergency Management Agency, http://www.fema.gov/library/viewRecord.do?id=1880.

[47] Federal Emergency Management Agency, "Hazard Mitigation Planning," Federal Emergency Management Agency, accessed September 14, 2013, http://www.fema.gov/multi-hazard-mitigation-planning.

operations and will realize the benefits above. In essence, local jurisdictions are arguably developing CIKR protection and resiliency plans if they are participating in hazard mitigation planning.

E. CONCLUSION

The limited information available related to implementing and defining critical infrastructure at the local Level supports the need for further research to answer the following questions:

1. Is there a need to develop definitions for assisting local governments to assess and identify CIKR?
2. What value do identifying Critical Infrastructure assets provide for local jurisdictions?
3. How do the federal, state and Local CIKR definitions intersect?

In a 2005 *Homeland Security Affairs* article, "Potholes and Detours in the Road to Critical Infrastructure Protection Policy," the authors suggest that "the federal government take greater responsibility (and control) over state and local decisions" related to CI.[48] While this may better develop federal CI asset lists and better address sectors with an interstate impact, it is important to remember that all responses to natural and manmade disasters begin at the local Level. Local jurisdictions should have an interest, and a voice in how they deploy resources, both physical and financial, in the protection of their communities. Conversely, local jurisdictions must understand the importance of protecting CIKR and developing resiliency plans with less reliance on state and federal governments. CIKR protection is a local problem.

[48] Ted G. Lewis and Rudy Darken, "Potholes and Detours in the Road to Critical Infrastructure Protection Policy," *Homeland Security Affairs*, 1, no. 2 (2005), http://www.hsaj.org/?article=1.2.1.

III. RESEARCH METHODOLOGY

A. RESEARCH METHOD

1. Objective

The purpose of this research was to conduct an analysis of the existing federal Critical Infrastructure and Key Resources Protection Program to determine the overall effectiveness and applicability of this program for identifying and protecting CIKR assets at the state and local Level, and to make recommendations for improvement. Furthermore, this research performed a case study of the state of New Hampshire model for identifying CIKR assets at the state Level.

2. Sample Selection

First, as the foundation for developing CIKR protection plans, the Department of Homeland Security (DHS) released the *National Infrastructure Protection Plan* in 2008 to address the national policy for critical infrastructure protection and key resource protection (CIKR) requirements as set forth in *Presidential Decision Directive 7 (PDD-7): Critical Infrastructure Identification, Prioritization, and Protection*.[49] PDD-7 identifies 18 sectors for CIKR and assigns each a "sector-specific agency," which is responsible for developing federal CIKR sector specific criteria. Secondly, the state of New Hampshire, via a subcommittee of the Governor's Advisory Council on Emergency Preparedness and Security (ACEPS), has reviewed the federal criteria for identifying CIKR assets and has developed definitions for defining assets that are critical to the state.[50] Lastly, an analysis of alternative community preparedness programs and state homeland security strategies was conducted to determine whether these methodologies can be applied to state and/or local CIKR protection programs.

[49] White House, *Presidential Decision Directive 7*.

[50] State of New Hampshire, Department of Safety, *State of New Hampshire Homeland Security CI/KR Identification Report* (restricted-access document).

3. Data Sources

Research data sources included the NIPP, government reports and state homeland security strategies. Furthermore, data was collected via an information request to each of New England states' Department of Homeland Security to gather data related to each state's homeland security strategy and state-specific critical infrastructure protection programs.

4. Analysis

Analysis included a review of the strengths and weaknesses of the NIPP as it relates to CIKR definitions at the state and local Level. Further analysis sought to identify the relationships between the sample selections and to identify potential gaps in the applicability to state and local CIKR protection planning. Furthermore, a case study of the state of New Hampshire CIKR program was performed to compare this program to the NIPP and the federal criteria for CIKR asset identification.

5. Output

Through process modeling this research sought to identify a model framework for developing a local CIKR protection program and defining assets that are critical to local jurisdictions.

B. RESEARCH LIMITATIONS

The analysis of relevant data included the need to review state homeland security strategies as the basis for data related to critical infrastructure protection planning efforts at the state Level. Upon searching the literature, there were a very limited number of state strategies available as open source documents. In an effort to maintain a manageable quantity of data, the New England region was selected. Additionally, research found no local CIKR protection planning strategies. Lastly, some data sources reviewed were labeled as "For Official Use Only" and therefore not open source documents. The author chose to purposely not include specific data related to these documents in an effort to maintain this thesis as an open source document.

IV. SUMMARY OF DATA

A. FEDERAL CRITICAL INFRASTRUCTURE PROTECTION PROGRAM

This section will review the criteria for assessing and prioritizing assets, systems, and networks for the federal sectors-specific plans (SSP) for the sectors identified in PPD-21 and the applicability of these criteria to State and local jurisdictions. The *Government Facilities Sector-Specific* plan has not been included as is not available as an open source document. Each of the SSP's utilizes the *National Infrastructure Protection Plan Risk Management Framework* for developing their respective sectors plan.

The *Risk Management Framework* lays the foundation for the steps in developing the sector specific plans. The key components are: setting goals and objectives; identify assets, systems, and networks; assess risk; prioritize assets, systems, and networks; implement programs; and measure effectiveness.[51]

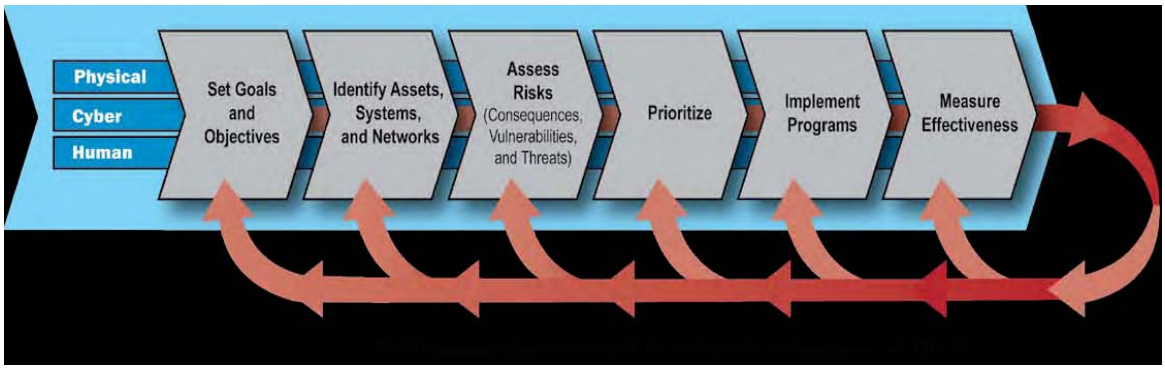

Figure 1. NIPP Risk Management Framework[52]

B. SETTING GOALS AND OBJECTIVES

The NIPP states, "Achieving robust, protected, and resilient infrastructure requires national, state, local, and sector-specific CIKR protection visions, goals, and

[51] U.S. Department of Homeland Security, *National Infrastructure Protection Plan*, 28.

[52] Ibid., 27.

objectives that describe the desired risk management posture."[53] Furthermore, the NIPP states that the risk management framework supports this goal by "enabling the development of the national, State, regional and sector risk profiles" and "enabling DHS, SSA's, and other partners to reduce the potential consequences, threats, or vulnerabilities to CIKR.[54]

C. IDENTIFY ASSETS, SYSTEMS, AND NETWORKS

The Department of Homeland Security maintains an inventory of the nation's CIKR assets, systems and networks.[55] Each sector-specific agency is responsible for working with owners and operators of CI, sector coordinating councils (SCC),[56] and other sources to develop the inventories of sector assets, systems and networks.[57] The individual sector lists are used to populate the nation's inventory of critical assets, networks, and systems. Other mechanisms described for developing CI inventories include: voluntary submittals; study results; ongoing reviews of high risk locations; and the DHS National Critical Infrastructure Prioritization Program (NICPP) data call.[58]

The NCIPP data call is an annual, voluntary request to state, territorial and Federal CIKR partners, in which CI assets, systems or networks are "nominated" for inclusion in the Federal inventory. [59] According to DHS, the main goals of the NCIPP are to: (1) identify infrastructure critical to the nation's public health and safety, economic, or national security; (2) better prioritize assets, systems, and networks so as to allow DHS to more efficiently allocate resources; and (3) focus planning, foster coordination, and

---

[53] Ibid., 28.

[54] Ibid.

[55] Ibid., 29.

[56] Sector Coordinating Council has self-organized membership and should be representative of a broad base of owners, operators, associations, and other entities—both large and small—within a sector. U.S. Department of Homeland Security, *National Infrastructure Protection Plan*, 55.

[57] Ibid., 30.

[58] Ibid.

[59] Ibid.

support preparedness efforts for incident management, response, and restoration activities by developing a collaborative relationships amongst all stakeholders.[60]

1. Assess Risk

The NIPP suggests that CIKR sectors assess risk in the context of consequence, vulnerability, and threat.

Risk = Consequence x Vulnerability x Threat

- Consequence can be viewed as the overall effects of an incident. [61] Typical examples can include loss of life or injuries, property loss, fear instilled in a population, or impact to government operations.
- Vulnerability can be defined as a weakness that could result in the success of any of the above consequences.
- Threat is often the most difficult to determine but can be defined as "natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property." [62]

Examples of threat can be specific intelligence related to an attack on a community or infrastructure or the forecast of a severe weather event to impact a community.

2. Prioritize Assets, Systems, and Networks

This process "involves aggregating, combining, and analyzing risk assessment results to determine which assets, systems, networks, sectors, or combinations of these face the highest risk so that risk management priorities can be established."[63] The NCIPP has developed criteria to prioritize high-risk federal assets, systems or networks as either Level 1 or Level 2 based on consequence in four areas: fatalities, economic loss, mass evacuation length, and degradation of national security.[64] In order for an asset, system or network to be included on the Level 1 or 2 lists it must meet two of the four consequence

[60] Government Accountability Office, *Critical Infrastructure Protection: DHS List of Priority Assets Needs to Be Validated and Reported to Congress* (GA0-13-296), 2013, Government Accountability Office, http://www.gao.gov/assets/660/653300.pdf.

[61] U.S. Department of Homeland Security, *National Infrastructure Protection Plan*, 32.

[62] Ibid.

[63] Ibid., 40.

[64] Government Accountability Office, *Critical Infrastructure Protection*, 4.

thresholds.[65] This process is somewhat subjective in how assets are placed on the federal CI list. The consequence thresholds in the federal data call are labeled "For Official Use Only" (FOUO) and will not be included in this thesis unless they have been included in open-source sector specific plans. The NCIPP also identifies Level 3 for sector specific CIKR lists and Level 4 for state and territory CIKR lists. The sector and states lists are used to identify CIKR, which are important to the sector or state but do not meet Levels 1 or 2 criteria.[66]

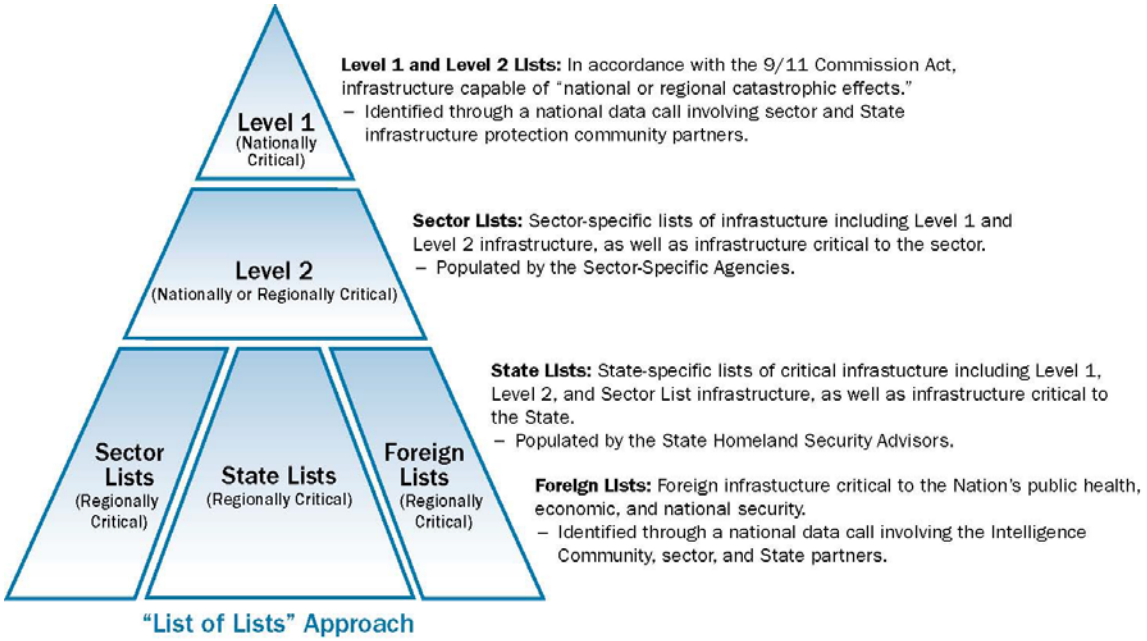

Figure 2. DHS List of Lists[67]

[65] Ibid., 14.

[66] U.S. Department of Homeland Security, *Food and Agriculture Sector Specific Plan*, 2010, U.S. Department of Homeland Security, http://www.dhs.gov/xlibrary/assets/nipp-ssp-food-ag-2010.pdf, 27.

[67] U.S. Department of Homeland Security, *Communications Sector-Specific Plan*, 2010, U.S. Department of Homeland Security, http://www.dhs.gov/xlibrary/assets/nipp-ssp-communications-2010.pdf, 39.

D. IMPLEMENT PROTECTIVE PROGRAMS AND RESILIENCY STRATEGIES

Protective programs and resiliency strategies are designed to reduce risk by: preventing, deterring, or mitigating threat; reducing vulnerabilities and minimizing consequences. The NIPP risk management framework focuses on efficient allocation of resources.[68] According to the NIPP, "effective protective programs and resiliency strategies must be comprehensive, coordinated, cost effective, and risk informed."[69] Programs should not only include physical security, but the cyber and human related elements of CIKR. Protective strategies can include: "implementing operational changes; physical protection; equipment hardening; cyber security; system resiliency; backup communications; response plans, training; and security upgrades."[70] Due to complex and geographically distributed assets, systems and networks, a collaborative program must include participation from CIKR owners and operators: state, local and tribal authorities; federal agencies and sector-specific agencies.[71] Cost-effective programs and strategies focus "actions that offer the greatest mitigation of risk per expenditure."[72] Risk-informed programs should attempt to mitigate of risk by limiting consequence. Consequence reduction can be accomplished by reducing loss, reducing vulnerability, and/or reducing threats.[73]

1. Measuring Effectiveness

Performance metrics are used to determine or evaluate the overall effectiveness of programs. The NIPP outlines metric types and progress indicators. Two metric types, output and descriptive data are suggested to evaluate programs. Output (or process) data are used "to determine whether specific activities were performed, track progress of

---

[68] U.S. Department of Homeland Security, *National Infrastructure Protection Plan*, 43.

[69] Ibid.

[70] Ibid.

[71] Ibid.

[72] Ibid, 44.

[73] Ibid.

tasks, or report the output of a process."[74] Descriptive data are "used to understand sector resources and activities."[75] Metric progress indicators "utilize sector priorities to monitor sector metrics and data."[76] Any or all of these measures will help to determine resource allocation and for the development of investment strategies.

E. FEDERAL CRITICAL INFRASTRUCTURE SECTOR-SPECIFIC PLANS

The following section briefly describes the scope of each sector, the strategy for develop sector-specific asset, system, and network lists and the methodology each sector identifies for collaborating with state and local partners. The criteria utilized varies widely from clear, concise consequence based as in the water sector to the reliance on owners and operators of CIKR or subject matter experts.

1. Chemical Sector

The chemical sector represents a "$689 billion business of chemistry" that can be divided into five areas: (1) basic chemistry—raw materials used in the manufacture or processes of products, (2) specialty chemicals—products produced in lower volumes used as the primary ingredient or as a processing aid in the manufacture of products, (3) agricultural chemicals—used primarily by farmers as fertilizer or crop protection, (4) pharmaceuticals—includes prescription and over the counter drugs and biotechnology, and (5) consumer products—packaged goods including, soap, detergents, hair and skin care products, cosmetics, and perfume.[77]

The primary method for collecting sector CIKR high-risk data is through the Chemical Facility Anti-Terrorism Standards (CFATS) regulatory program. CFATS requires operators of high risk chemical facility to perform security assessments identify vulnerabilities, and develop security plans.[78] The *Chemical Sector-Specific Plan* has

---

[74] Ibid., 47.

[75] Ibid.

[76] Ibid.

[77] U.S. Department of Homeland Security, *Chemical Sector-Specific Plan*, 2010, U.S. Department of Homeland Security, http://www.dhs.gov/xlibrary/assets/nipp-ssp-chemical-2010.pdf, 99–100.

[78] Ibid., 38.

developed the following criteria for identifying Level 1 and Level 2 CIKR based on the criteria developed by the NCIPP (see Table 1).

NCIPP Level 1	NCIPP Level 2
Those CIKR that, if disrupted, could result in at least two of the following consequences:	Those CIKR that, if disrupted, could result in at least two of the following consequences:
1. Greater than 5,000 prompt fatalities. 2. Greater than $75 billion in first-year economic consequences. 3. Mass evacuations with a prolonged absence of greater than 3 months. 4. Severe degradation of the country's national security capabilities, including intelligence and defense functions, but excluding military facilities.	1. Greater than 2,500 prompt fatalities. 2. Greater than $25 billion in first-year economic consequences. 3. Mass evacuations with a prolonged absence of greater than 1 month. 4. Severe degradation of the country's national security capabilities, including intelligence and

Table 1. Criteria for NCIPP Level 1 and Level 2 CIKR[79]

Throughout the plan the role of state governments is emphasized. Specifically, the sector utilizes the State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC) "to engage State representatives and maintains particularly focused dialogue with States regulating the security of chemical facilities in their jurisdiction."[80] The plan emphasizes the role of state, local, tribal, and territorial authorities as being critical to CI protection. They constitute "the front line of defense in preventing harm and providing response when necessary to secure the chemical sector's critical infrastructure through public safety agencies such as local law enforcement, fire and rescue, emergency medical services, and emergency management."[81] The chemical sector plan states that this sector has a history of working emergency responders and regulators at the state and local Level, but there is no evidence cited to support the effectiveness of this effort.

2. Commercial Facilities Sector

The commercial facilities sector represents eight sub-sectors that have a significant influence on the nation's economy. For example, "the retail industry

[79] Ibid., 39.

[80] Ibid., 19.

[81] Ibid., 25.

conducted more than $4.6 trillion in annual sales in 2008, has more than 1.6 million U.S. establishments and more than 24 million employees."[82] Additionally, the hotel industry generated $139.4 billion due to tourist and business travel in 2007, and commercial casinos paid more than $5.7 billion in direct gaming taxes in 2008.[83] Subsectors include:

- **Entertainment and media**—media production, print media and broadcast media.
- **Gaming facilities**—casinos and the facilities associated with the, such as, hotels, conference centers, and shopping centers.
- **Lodging**—non-gaming resorts, hotels and motels, hotel-based conference centers, and bed-and-breakfast establishments.
- **Outdoors events—**amusement parks, fairs, exhibitions and parks.
- **Public assembly**—convention centers, auditoriums, stadiums, arenas, movie theaters, cultural properties, and other assets where large numbers of people congregate.
- **Real estate**—office buildings and office parks, apartment buildings, multi-family towers and condominiums, self-storage facilities, and property management companies.
- **Retail—**enclosed malls, shopping centers, strip malls, and freestanding retail establishments.
- **Sports leagues**—major sports leagues and federations and a sports broadcasting network.[84]

Criteria for identifying assets, systems, and networks references the federal data call but does not list these in the sector-specific plan. The sector uses "consequence-based" criteria (e.g., loss of life, economic impact, mission disruption) for developing the various Level 1/Level 2 asset lists.[85] The primary consequence utilized is loss of life, and then economic impact.[86] Each subsector also uses "unique features" to nominate the asset, system, or network for inclusion as NICPP Level 1 or Level 2 CIKR. For example, lodging includes the "location of the property, clientele, proximity to high-risk

[82] U.S. Department of Homeland Security, *Commercial Facilities Sector-Specific Plan*, 2010, U.S. Department of Homeland Security, http://www.dhs.gov/xlibrary/assets/nipp-ssp-commercial-facilities-2010.pdf, 7.

[83] Ibid.

[84] Ibid., 8–9.

[85] Ibid., 36.

[86] Ibid., 37.

enterprises, or the iconic status of the hotel."[87] Public assembly lists the "size of the facility, amount of space or the occupancy load" as sector specific attributes.[88]

There are numerous references to the importance of state and local government agencies involvement in identifying assets, systems, and networks. The plan states:

> State and local first responders, emergency managers, public health officials, and others involved in homeland security missions frequently interact with Critical Facilities Sector owners and operators in their jurisdictions to plan for and respond to all manner of natural and manmade hazards.[89]

3. Communications Sector

The communications sector is a network of complex wired, wireless, broadcast, cable and satellites that delivers critical communications services throughout the United States. Services include: telephone; cellular; radio and television; paging, data, and voice services; and public safety communications systems.[90]

The communications sector identifies assets, systems, and networks by accepting nominations from any of the following:[91]

- *Industry*—private sector owners of communications CIKR and industry partners that are dependent on communications for the delivery of services;
- *Manager/Director of the National Communications System (NCS)*;
- *National Communications System Committee of Principals and Council of Representatives*—responsible for designating critical government assets or critical and essential operations;
- *Cross-Sector Communications Dependencies*—the sector uses "the combined cross-sector lists of Level 1 and Level 2 CIKR to determine supporting communications facilities as follows":

[87] Ibid., 91.

[88] Ibid., 104.

[89] Ibid., 25.

[90] U.S. Department of Homeland Security, *Communications Sector-Specific Plan*, 12.

[91] Ibid., 38.

- Three or more Level 1 or Level 2 CIKR through one communications facility,
- Nominated assets as designated by the sector:
  - *Emergency Services*—includes Public Safety Answering Points (PSAP) and the Emergency Alert System (EAS) as nominated by the Federal Communications Commission (FCC), DHS Protective Security Advisors or Emergency Support Function Communications representatives;
  - *High Capacity Assets*—Major switching centers, major underwater cable landings or telecommunications "hotels;"
  - *Automatic Inclusion*—credible threats and national security implications are automatically included in the sector list.

Assets, systems, and networks are prioritized using a consequence based risk criteria but the sector is moving to a risk-based process.[92] Communications assets are determined to be critical based on location and the effects on end users in the incident impact area.[93] The sector link to local jurisdictions is stated in goal three of the sector-specific plan as "improving the sector's national security and emergency preparedness (NS/EP) posture with federal, state, local, tribal, international, and private sector entities to reduce risk."[94] State and local sector relationships include: regulatory issues with state public utilities commissions, state and local emergency operations centers, and with first responders and 911 centers.[95]

4. Critical Manufacturing

The critical manufacturing sector includes several different processes that produce products and materials. This sector is broken into four areas: primary metals manufacturing; machinery manufacturing; electrical equipment manufacturing; and transportation and heavy equipment manufacturing.[96] Sector partners include: federal

[92] Ibid., 35.

[93] Ibid., 36.

[94] Ibid., 3.

[9595] Ibid., 15.

[96] U.S. Department of Homeland Security, *Critical Manufacturing Sector-Specific Plan*, 2010, U.S. Department of Homeland Security, http://www.dhs.gov/xlibrary/assets/nipp-ssp-critical-manufacturing-2010.pdf, 9.

agencies, state, local, tribal and territorial governments; private sector owners and operators; advisory councils; and academia, research centers and think tanks.[97]

Assets, systems, and networks are determined by a sector-wide risk assessment process with voluntary participation and input from sector partners.[98] The sector plan states the following related to prioritizing CIKR, "The sector prioritization process will involve aggregating, combining, and analyzing risk-assessment results to determine which assets or systems face the highest risk (i.e., the most critical assets/systems)."[99] The prioritization process fundamentally first identifies critical assets and second determines how to provide the best and most cost-effective protective actions.

The *Critical Manufacturing Sector Plan* states, "State, local, tribal and territorial authorities are integral to protecting our nation's infrastructure and are the front line of defense for our nation's infrastructure and serve as or in close proximity to the owners or operators of CIKR."[100] Some evidence of engagement of state and local emergency planners is the efforts of this sector to participate in local emergency planning activities, such as hazardous materials incident planning.

5. Dams

The dams sector includes dam projects, hydropower generation facilities, navigation locks, levees, dikes, hurricane barriers, mine tailings and other industrial waste impoundments, and other similar water retention and water control facilities.[101] Dams serve a number of purposes including: holding back water; impounding water to create a reservoir; creating spillways to control flood waters; housing equipment to produce electricity, and creating canals or aqueducts to move water or provide a navigational waterway (see Figure 3).[102]

---

[97] Ibid., 12–16.

[98] Ibid., 25–26.

[99] Ibid., 32.

[100] Ibid.

[101] U.S. Department of Homeland Security, *Dams Sector-Specific Plan*, 2010, U.S. Department of Homeland Security, http://www.dhs.gov/xlibrary/assets/nipp-ssp-dams-2010.pdf, 11.

[102] Ibid., 14.

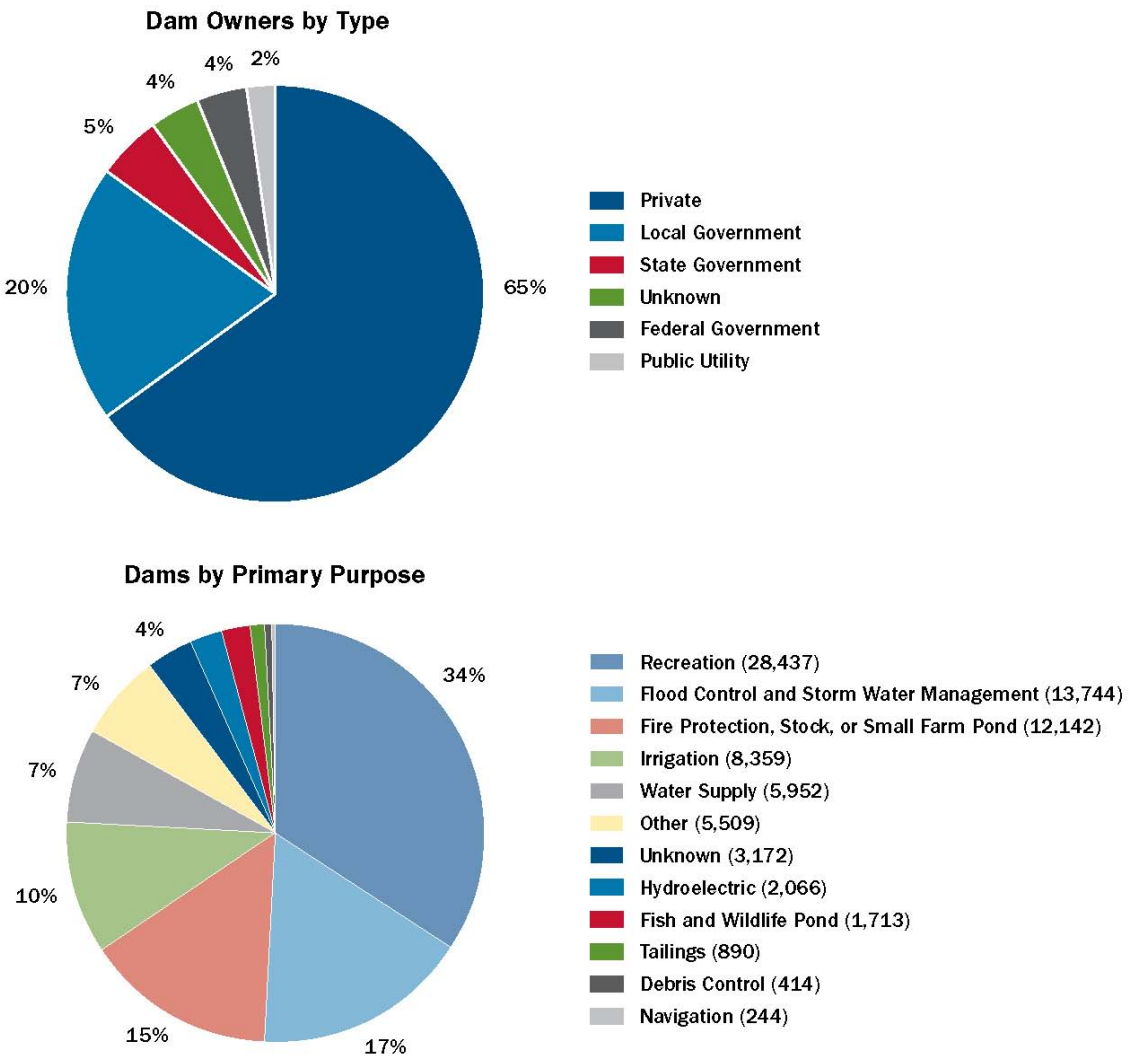

Figure 3. Dam Ownership and Purpose of U.S. Dams[103]

According to the *Dams Sector Plan*, the "Dams Sector has long-standing and well-established programs to assess, mitigate, and respond to the potential damages caused by catastrophic dam failures induced by natural hazards."[104] There are competing ideas related to risk assessment within the dams sector due to a lack of consensus

[103] Ibid., 16.

[104] Ibid., 52.

between dam owners and regulators on a risk assessment methodology.[105] The sector currently utilizes the consequence-based top screen (CTS) methodology to prioritize assets based on consequences (see Table 2).

Consequence Category	Consequence Parameter	Measurement Unit
Human Impacts	Total Population at Risk (PAR)	Number of people
	PAR 0–3 miles	Number of people
	PAR 3–7 miles	Number of people
	PAR 7–15 miles	Number of people
	PAR 15–60 miles	Number of people
Economic Impacts	Asset Repair/Replacement Cost	Millions of dollars
	Remediation Cost	Millions of dollars
	Business Interruption Cost	Millions of dollars/year
Impacts on Critical Functions	Water Supply: Population Served	Number of people
	Irrigation: Annual Water Deliveries	Millions of dollars/year Acre-feet/year
	Hydropower Generation: Total Installed Capacity	Megawatts
	Flood Damage Reduction: Annual Damages Prevented	Millions of dollars/year
	Inland Navigation: Annual Navigation Tonnage	Kilotons/year
	Recreation: Annual Recreational Visitors	Number of people/year

Table 2. Consequence-Based Top Screen Parameters[106]

According to the *Dams Sector Plan*, state governments are responsible for 84 percent of the dams on the national inventory of dams and are represented by eight state dam safety officials on the Sector Government Coordinating Council. Local governments, public utilities, levee districts and water management districts own and operate dams and levees are represented largely by professional organizations.[107]

[105] Ibid., 53.

[106] Ibid., 45.

[107] Ibid., 29.

6. Defense Industrial Base Sector

The defense industrial base (DIB) sector consists of government and private sector organizations that support military operations. Sector functions include: research and development; system design and manufacture; and the design, development, delivery and maintenance of military weapons systems.[108] The sector focuses on "mission critical tasks" or the impact to defense missions to analyze and prioritize assets, systems, and networks. The criteria for screening priorities includes: "Single source suppliers, sole source or defense-unique suppliers; suppliers of dual-use products; suppliers of products used in multiple programs; suppliers with high requalification costs or long requalification timeframes; and suppliers developing advanced or emerging technology" (Figure 4).[109]

[108] U.S. Department of Homeland Security, *Defense Industrial Base Sector-Specific Plan*, 2010, U.S. Department of Homeland Security, http://www.dhs.gov/xlibrary/assets/nipp-ssp-defense-industrial-base-2010.pdf, 15.

[109] Ibid., 23–24.

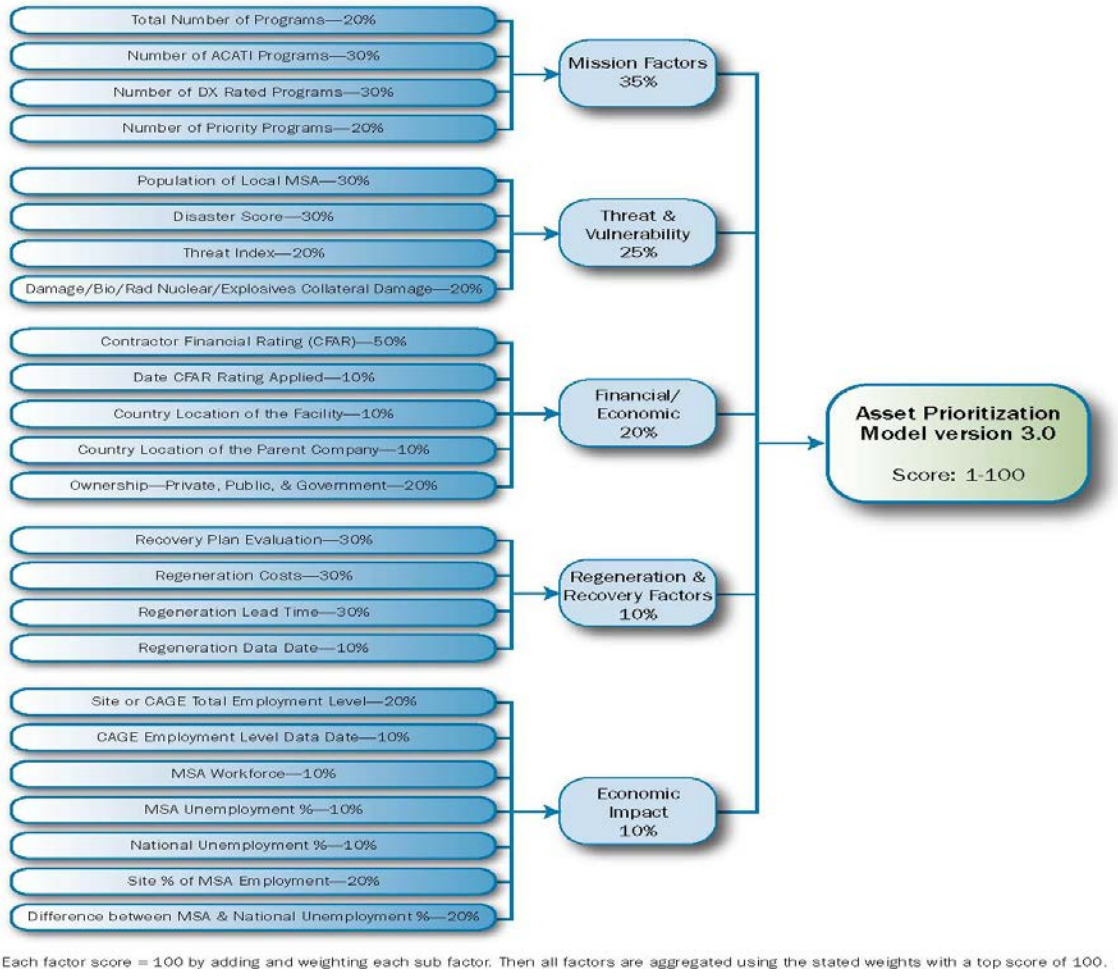

Figure 4. Prioritization Factors, Sub Factors, and Weights[110]

The sector plans states a sector goal related to risk management as to "use an all-hazards approach to manage the risk-related dependency on critical DIB assets."[111] One objective related to this goal is to "improve the effectiveness of government threat reporting to officials, owners and operators responsible for critical defense industrial base assets, local law enforcement, and other first responders."[112]

[110] Ibid., 36.

[111] Ibid., 19.

[112] Ibid., 19.

7. Emergency Services Sector

The primary mission of the emergency services sector (ESS) is to "save lives, protect property and the environment, assist communities impacted by disasters and aid recovery during emergencies." The ESS is made up of five disciplines: law enforcement; fire and emergency services; emergency management; emergency medical services; and public works within each discipline there are a number of specialized capabilities (e.g., hazardous materials, search and rescue, explosive ordinance disposal, special weapons and tactics and tactical operations, aviation).[113] The scope of this sector includes a vast number of facilities, equipment and trained personnel, spread over a large, geographic area.[114]

The ESS utilizes the "Target Capabilities List" (2007), now known as the "Core Capabilities List" in the *National Preparedness Goal* (see Table 3) to develop sector goals and collect information.[115] ESS assets, systems, and networks consist of equipment and materials, vehicles, facilities and data records, access control and data collection systems, control systems, and strategically trained personnel, and mutual aid and multi-agency coordination.[116] The ESS plan states, "there are three general risk assessment layers: (1) facility-specific or fixed assets, (2) specialized emergency services assets or systems, and (3) multiple systems in a region or multiple regions."[117] The plan does not outline a specific methodology for identifying or assessing the risk to assets, networks, and systems.

---

[113] U.S. Department of Homeland Security, *Emergency Services Sector-Specific Plan*, 2010, U.S. Department of Homeland Security, http://www.dhs.gov/xlibrary/assets/nipp-ssp-emergency-services.pdf, 11–12.

[114] Ibid., 2.

[115] Ibid., 31.

[116] Ibid., 32–33.

[117] Ibid., 45.

Prevention	Protection	Mitigation	Response	Recovery
Planning				
Public Information and Warning				
Operational Coordination				
Forensics and Attribution Intelligence and Information Sharing Interdiction and Disruption Screening, Search, and Detection	Access Control and Identity Verification Cyber security Intelligence and Information Sharing Interdiction and Disruption Physical Protective Measures Risk Management for Protection Programs and Activities Screening, Search, and Detection Supply Chain Integrity and Security	Community Resilience Long-term Vulnerability Reduction Risk and Disaster Resilience Assessment Threats and Hazard Identification	Critical Transportation Environmental Response/ Health and Safety Fatality Management Services Infrastructure Systems Mass Care Services Mass Search and Rescue Operations On-scene Security and Protection Operational Communications Public and Private Services and Resources Public Health and Medical Services Situational Assessment	Economic Recovery Health and Social Services Housing Infrastructure Systems Natural and Cultural Resources

Table 3. Core Capabilities List[118]

The ESS plan identifies the importance of engaging state, local, tribal, and territorial governments in the development of the sector-plan and asset, system, and network identification. Furthermore, the plan states:

> …responsibility for incident management initially falls on State, local, tribal, and territorial authorities, but the majority of ESS disciplines are

[118] U.S. Department of Homeland Security, *National Preparedness Goal*, 2011, Federal Emergency Management Agency, http://www.fema.gov/pdf/prepared/npg.pdf.

> organized and provided at the local Level of government by career and volunteer personnel from the communities.[119]

This statement is consistent with the roles and responsibilities of emergency response in the National Incident Management System.

8. Energy Sector

The energy sector "consists of thousands of electricity, oil, and natural gas assets that are geographically dispersed and connected by systems and networks" (see Table 4).[120] Energy assets and critical infrastructure are owned by private, federal, state, and local entities, as well as some large industries and financial institutions.[121] The scope of this sector is very large and each subsector has some reliance on other subsectors. For example, 70percent of the electrical generation is provided by fossil fuels (coal, natural gas or oil).[122] A 2008 inventory of the electricity subsector shows that there are: 6,413 power plants; 30,320 substations; 6,222 miles of high voltage DC transmission lines, and 143 million customers.[123] The petroleum subsector includes: 525,000 producing wells, 150 refineries, and 1,400 petroleum terminals.[124] The natural gas subsector is comprised of: 478,562 gas and condensate wells; over 500 gas processing plants; and approximately 1.5 million miles of pipelines (see Table 4).[125]

---

[119] Ibid., 25.

[120] U.S. Department of Homeland Security, *Energy Sector-Specific Plan*, 2010, U.S. Department of Homeland Security, http://www.dhs.gov/xlibrary/assets/nipp-ssp-energy-2010.pdf, 2.

[121] Ibid., 9

[122] Ibid., 10.

[123] Ibid., 11.

[124] Ibid., 13.

[125] Ibid., 16.

Electricity	Petroleum	Natural Gas
• Generation – Fossil Fuel Power Plants » Coal » Natural Gas » Oil – Nuclear Power Plants[a] – Hydroelectric Dams[a] – Renewable Energy • Transmission – Substations – Lines – Control Centers • Distribution – Substations – Lines – Control Centers • Control Systems • Electricity Markets	• Crude Oil – Onshore Fields – Offshore Fields – Terminals – Transport (pipelines)[a] – Storage • Petroleum Processing Facilities – Refineries – Terminals – Transport (pipelines)[a] – Storage – Control Systems – Petroleum Markets	• Production – Onshore Fields – Offshore Fields • Processing • Transport (pipelines)[a] • Distribution (pipelines)[a] • Storage[b] • Liquefied Natural Gas Facilities[b] • Control Systems • Gas Markets

[a] Hydroelectric dams, nuclear facilities, rail, and pipeline transportation are covered in other SSPs.

[b] Certain infrastructure of this asset type are regulated by the Chemical Facility Anti-Terrorism Standards (CFATS). The final tiering of the facilities covered by the CFATS was not completed at the time of this report.

Table 4. Segments of the Energy Sector[126]

The energy sector has identified six characteristics to assist in identifying assets, systems, and networks: physical and location features; cyber, volume or throughput, demands for energy, human attributes, and importance of asset to the system or network.[127] The sector relies on the owners and operators for prioritization of assets and networks. The plan states "from a grid perspective, the nation's oil and natural gas pipeline systems and electricity grid are designed and operated with built-in redundancy to ensure a certain degree of reliability and resilience."[128]

The *Energy Sector Plan* lists the following goal: "clearly define critical infrastructure protection roles and responsibilities among all Federal, State, local, and private sector partners."[129] Furthermore, the plan identifies state and local governments as "crucial stakeholders" in providing secure and reliable energy to the nation.[130] Lastly,

[126] Ibid., 9

[127] Ibid., 27.

[128] Ibid., 39.

[129] Ibid., 2.

[130] Ibid., 22.

the plan suggests that to successfully identify the risk to this sector and protect assets, systems, and networks, State and local jurisdictions must work with sector owners and operators to understand which facilities are critical.[131]

9. Food and Agriculture Sector

The food and agriculture sector provides food for human and animal consumption and includes a system of production, processing, and delivery. According to the sector plan, the United States has approximately 44,000 food processors, 113,000 food warehouses, 2.2 million farms, and over 1.2 million retail food facilities and accounts for about one-fifth of the nation's economy.[132]

The food and agriculture sector utilizes two mechanisms to define and identify critical assets within the sector: 1) the annual federal data call, and 2) the Food and Agriculture Sector-Criticality Assessment Tool (FAS-CAT).[133] FAS-CAT was developed by the National Center for Food Protection and Defense (NCFPD) to assist with the definition, identification, collection, verification, and updating of infrastructure information. The food and agriculture sector plan states the purpose of FAS-CAT is "to assist States in determining and documenting the most critical elements, systems, and subsystems in the FA Sector infrastructure at the state Level."[134] There have been some difficulties in collecting information: 1) the sector focuses on systems versus individual assets and 2) States are not uniformly reporting their list of assets.[135] Assets that are collected are prioritized by using consequence based metrics. The following is listed as the criteria for prioritizing assets:

> …duration of disruption; complete destruction of facilities; relationship to the commodity being produced (i.e., loss of acreage of corn fields versus loss of entire specific product); ability of adjacent and nearby facilities to

[131] Ibid., 40.

[132] U.S. Department of Homeland Security, *Food and Agriculture Sector Specific Plan*, 9–10.

[133] Ibid., 24.

[134] Ibid.

[135] Ibid., 26.

> adequately compensate for the loss of production or service; financial markets; and CIKR supporting response and recovery.[136]

The *Food and Agriculture Sector Plan* references state and local jurisdiction largely in relation to food protection and agriculture agencies that have jurisdiction over the food supply at the retail and wholesale Levels. State and local agencies are responsible for "the inspection and oversight of over one million food establishments—restaurants and grocery stores, vending machines, cafeterias, and other outlets in health care facilities, schools, and correctional facilities."[137] The plan further states a goal as to:

> …work with State and local entities to ensure that they are prepared to respond to incidents. The sector will ensure that the combined Federal, State, local, and, tribal capabilities are prepared to respond quickly and effectively to a terrorist attack, major disease outbreak, or other disaster affecting the national food and agriculture infrastructure.[138]

10. Finance and Banking Sector

The banking and finance sector describes the sector as "groups of products and services, which are: (1) deposit, consumer credit, and payment systems; (2) credit and liquidity products; (3) investment products; and (4) risk-transfer products (including insurance)."[139] The financial services sector includes "more than 18,800 federally insured depository institutions; thousands of providers of various investment products, including roughly 18,440 broker-dealer, investment advisers, and investment company complexes; and 7,948 domestic U.S. insurers."[140]

According to the *Banking and Finance Sector-Specific Plan* risk assessments are largely directed to address the interdependencies between this sector and others, such as energy, transportation, communications or information technology.[141] Risk assessment is

---

[136] Ibid., 40.

[137] Ibid., 19.

[138] Ibid., 20.

[139] U.S. Department of Homeland Security, *Banking and Finance Sector-Specific Plan*, 2010, U.S. Department of Homeland Security, https://www.dhs.gov/sites/default/files/publications/nipp-ssp-banking-and-finance-2010.pdf, 1.

[140] Ibid., 8.

[141] Ibid., 16.

primarily based on consequences related to the sectors ability to operate efficiently and the impact on public confidence in the financial system.[142] The plan does not adequately define "public confidence" or state how this can be measured. Assets are prioritized based on the following factors:

> …degree of dependence on the asset; presence or absence of alternative suppliers; public need for the services; potential impact of a disruption to the financial system; potential impacts on the economy through the cascading disruption of other CIKR; and trends and specific information in threat analysis.[143]

The *Banking and Finance Sector-Specific Plan* promotes collaboration through "regional coalitions to build relationships and share information among financial institutions and first responders, emergency management personnel, and officials at the local Level." [144] However, the plan does not define the make-up of these coalitions. The role of the Financial and Banking Information Infrastructure Committee (FBIIC) is to "promote information sharing among and between the Federal, State, local, and tribal authorities, as well as the private sector."[145] In addition the role of the Treasury Department is to "protective response planning exercises designed to protect CIKR, and to create a response plan that incorporates State, local, and tribal law enforcement; and Enhancing communication and coordination across the sector."[146]

11. Healthcare and Public Health Sector

The health care subsector encompasses mostly private owned and operated organizations that deliver healthcare goods and services. The United States Department of Health and Human Services estimates that this subsector represents 16.2 percent or $2.2 trillion of the nation's gross domestic product in 2007.[147] The public health

---

[142] Ibid., 12.

[143] Ibid., 24.

[144] Ibid., 1.

[145] Ibid., 13.

[146] Ibid., 12.

[147] U.S. Department of Homeland Security, *Health Care and Public Health Sector-Specific Plan*, 2010, U.S. Department of Homeland Security, http://www.dhs.gov/xlibrary/assets/nipp-ssp-healthcare-and-public-health-2010.pdf, 9.

subsector includes federal, state, local, tribal, and territorial government entities that deals with the health of the population and has a role in large-scale disaster preparedness (see Table 5).[148]

Major Element	Private Sector	Public Sector			
		Federal	State	Local	Tribal
Healthcare personnel	> 13,000,000	> 450,000[a]			
Hospitals	3,905[b]	213[c]	1,105[d]		44[e]
Ambulatory healthcare services	~545,000 (unable to separate by ownership)[f]				
Nursing and residential care facilities	~75,000 (unable to separate by ownership)[g]				
Retail pharmacies	~42,000[h]				
Health departments		Parts of Federal departments and agencies, including HHS, Environmental Protection Agency, DoD, and VA	57	~3,000	36
Pharmaceutical manufacturers	~1,100[i]				
Medical device and supply companies	~ 2,500[j]				
Blood and organ banks	~1,200[k]				
Health insurers and other payers	>1,300[l]	1	50		

[a] See HHS, Health Resources and Services Administration, The Public Health Workforce Enumeration, **http://ask.hrsa.gov/detail_materials.cfm?ProdID=1057**.
[b] See American Hospital Association 2008 Survey Statistics.
[c] Ibid.
[d] Ibid.
[e] See Indian Health Services 2009 Fact Sheets.
[f] See U.S. Census Bureau, 2007 Economic Census, **http://www.census.gov/econ/census07**.
[g] Ibid.
[h] Ibid.
[i] Pharmaceutical manufacturers include pharmaceutical preparation manufacturers and medicinal and botanical manufacturers. See U.S. Census Bureau, 2007 Economic Census, **http://www.census.gov/econ/census07**.
[j] See U.S. Census Bureau, 2007 Economic Census, **http://www.census.gov/econ/census07**.
[k] Ibid.
[l] See America's Health Insurance Plans Association, **www.ahip.org**.

Table 5. Healthcare and Public Health Statistics[149]

The healthcare and public health sector utilizes the Risk Assessment Work Group (RAWG), a group of sector wide experts, to develop sector criteria definitions. The RAWG "analyzes critical functions in the sector which, if disrupted, would lead to overall mission degradation and cascading consequences. The group then identifies asset

[148] Ibid.

[149] Ibid., 11.

types that support these critical functions and their associated attributes."[150] The RAWG uses the information to develop scenarios that could impact the sector or the sectors ability to deliver health care services.[151] According to the *Sector-Specific Plan*, prioritizing of critical assets, networks, and systems has yet to be completed, but the plan outlines the following as the goal for accomplishing this.[152]

> In the broad range of healthcare and public health sector assets, systems, and networks that have been identified, certain infrastructure components would lead to the most severe consequences if compromised. After these components have been identified, an organization will be better equipped to prioritize resources and activities to protect the sector. This is the step for prioritizing infrastructure: Prioritize hazards and critical infrastructure based on probability and consequence.[153]

The *Healthcare and Public Health Sector-Specific Plan* states that state and local jurisdictions are represented on the Sector Government Coordinating Council. The Department of Health and Human Services, as the sector lead, is responsible for "working through two major State and local healthcare and public health professional associations to establish appropriate links with State, local, and territorial public health entities."[154]

12. Information Technology Sector

The information technology (IT) sector is comprised of physical assets and virtual systems and networks that provide "key capabilities and services" to the public and private sectors.[155] The *IT Sector-Specific Plan* identifies six critical functional areas that affect the sector's ability to provide IT services: incident management capabilities; domain name resolution services; identity management and associated trust support

---

[150] Ibid., 20.

[151] Ibid., 24.

[152] Ibid., 28.

[153] Ibid.

[154] Ibid., 14.

[155] U.S. Department of Homeland Security, *Information Technology Sector-Specific Plan*, 2010, U.S. Department of Homeland Security, https://www.hsdl.org/?abstract&did=7899, 1.

services; Internet-based content, information, and communications services; and, Internet routing, access, and connection services.[156]

The IT sector utilizes the NIPP *Risk Management Framework* for identifying sector assets, systems, and networks but largely relies on the subject matter experts assess sector assets, networks, and systems.[157] IT sector risk reduction and prioritization strategies focus on functions that would have the greatest impact on sector capabilities based on feedback from the subject matter experts (Table 6).[158]

[156] Ibid.

[157] Ibid., 21.

[158] Ibid., 30.

IT Sector Critical Function	Risks of Concern
Produce and provide IT products and services	Production or distribution of untrustworthy critical product or service through a successful manmade deliberate attack on a supply chain vulnerability.
Provide domain name resolution services	Breakdown of a single interoperable Internet through a manmade attack, and resulting failure of governance policy; large-scale manmade Denial-of-Service attack on the DNS infrastructure.
Provide Internet-based content, information, and communications services	Manmade unintentional incident caused in Internet content services results in a significant loss of e-Commerce capabilities.
Provide Internet routing, access, and connection services	Partial or complete loss of routing capabilities through a manmade deliberate attack on the Internet routing infrastructure.
Provide incident management capabilities	Impact to detection capabilities because of a lack of data availability resulting from a natural threat.

Table 6. IT Sector Risk Profile[163]

[163] Ibid. 26.

The *IT Sector-Specific Plan* identifies the importance of collaboration with State and local jurisdictions in the development of the sector plan. The plan states, "By working together, private and public IT Sector partners can prioritize protective initiatives and investments within and across sectors."[164] Collaboration will help to ensure efficient allocation of resources. According to the plan, states are represented through the National Association of Chief Information Officers and local governments through the SLTTGCC.[165]

13. Nuclear Sector

The nuclear sector is comprised of nuclear power plants; research, training and test reactors; deactivated nuclear facilities; fuel cycle facilities; nuclear materials transport; radioactive materials; radioactive source production and distribution facilities; and nuclear waste.[166] The most visible assets within the sector are 104 nuclear power plants and 32 research and test reactors, but radioactive materials are used "tens of thousands" of times each day for medical, research and industrials uses (Table 7).[167]

[164] Ibid., 1.

[165] Ibid., 13.

[166] U.S. Department of Homeland Security, *Nuclear Reactors, Materials and Waste Sector-Specific Plan*, 2010, U.S. Department of Homeland Security, http://www.dhs.gov/xlibrary/assets/nipp-ssp-nuclear-2010.pdf, 9.

[167] Ibid., 12

Nuclear Power Plants:
- Boiling water reactors (BWR); and
- Pressurized water reactors (PWR).

Research, Training, and Test Reactors:
- Government research and test reactors;
- University research and training reactors; and
- Private research and test reactors.

Decommissioned Nuclear Facilities:
- Deactivated reactors; and
- Other deactivated nuclear facilities.

Fuel Cycle Facilities:
- Uranium mining or in situ uranium leaching;
- Uranium ore milling or leachate processing;
- Uranium conversion facilities;
- Uranium enrichment facilities;
- Fuel fabrication facilities:
  - Category I (special nuclear materials) facilities;
  - Category II (special nuclear materials—moderate strategic significance) facilities; and
  - Category III (special nuclear materials—low strategic significance) facilities.

Nuclear Materials Transport:
- Low-hazard radioactive materials transport; and
- High-hazard radioactive materials transport.

Radioactive Materials:
- Medical facilities with radioactive materials;
- Research facilities using radioactive materials;
- Irradiation facilities; and
- Industrial facilities with nuclear materials.

Radioactive Source Production and Distribution Facilities:
- Radioactive device manufacturers;
- Radioactive source producers;
- Radioactive source importers; and
- Radioactive source manufacturers.

Nuclear Waste:
- Low-level radioactive waste processing and storage facilities;
- Sites managing accumulations of naturally occurring radioactive materials (NORM);
- Spent nuclear fuel processing and storage facilities:
  - Spent nuclear fuel wet storage facilities; and
  - Spent nuclear fuel dry storage facilities;
- Transuranic waste processing and storage facilities;
- High-level radioactive waste storage and disposal facilities; and
- Mixed waste processing.

Table 7. Nuclear Sector Taxonomy[168]

The nuclear sector is heavily regulated and must comply with numerous statutory requirements. This makes asset, system, and network identification information readily available for the development of the sector plan. The sector does not require states to submit federal data call Level 1 or Level 2 asset information but, it does coordinate with

[168] Ibid., 13

state and local jurisdictions to identify, request and use nuclear CIKR information.[169] Nuclear CIKR assets, systems, and networks are prioritized based on the potential radiological consequences associated with an attack.[170]

The *Nuclear Sector-Specific Plan* places a large emphasis on collaborating with state and local jurisdictions in the protection and resiliency of nuclear CIKR. However, as stated below, the relationship appears to be mostly tied to state representation and information sharing.[171]

> The Nuclear Regulatory Commission (NRC) looks to the State liaison officers to: (1) provide the primary communications channels between the States and the NRC; (2) serve as the key members in the States to keep the governors informed on issues under NRC's jurisdiction; and (3) provide the NRC with State information on particular nuclear safety, security, emergency, or environmental issues.

The plan does offer some information related to emergency planning zones, which can be utilized by state and local jurisdictions for emergency planning to assess the potential consequences associated with a radioactive material release.[172]

14. Transportation Systems Sector

The transportation sector is comprised of six subsectors: aviation; freight rail; highway; maritime; mass transit and passenger rail; and pipelines. According to the sector plan, transportation is responsible for the movement, distribution, and delivery of billions of passengers and millions of tons of good each year (Table 8).[173]

---

[169] Ibid. pp. 43–46

[170] Ibid., 66

[171] Ibid., 34

[172] Ibid., 55

[173] U.S. Department of Homeland Security, *Transportation Systems Sector-Specific Plan*, 2010, U.S. Department of Homeland Security, http://www.dhs.gov/xlibrary/assets/nipp-ssp-transportation-systems-2010.pdf, 18.

Aviation	Comprised of aircraft, air traffic control systems, and approximately 450 U.S. commercial airports and 19,000 public airfields. This mode includes civil and joint-use military airports, helipads, short take-off and landing ports, and seaplane bases.
Freight Rail	Consists of seven major carriers, hundreds of smaller railroads, over 140,000 miles of active railroad, over 1.3 million freight cars, and roughly 20,000 locomotives. Over 12,000 trains are operating per day. The Department of Defense has designated 30,000 miles of track and structure as critical to the mobilization and re-supply of U.S. Forces.
Highway and Motor Carriers	Encompasses more than four million miles of roadways and associated infrastructure such as, 600,000 bridges and tunnels, which carry vehicles including automobiles, school buses, motorcycles, and all types of trucks, trailers, and recreational vehicles.
Maritime	Includes a wide range of watercraft and vessels and consists of approximately 95,000 miles of coastline, 361 ports, more than 10,000 miles of navigational waterways, 3.4 million square miles of the Exclusive Economic Zone, and intermodal landside connections, which allow the various modes of transportation to move people and goods, to, from, and on the water.
Mass Transit and Passenger Rail	Includes multiple-occupancy vehicles, such as transit buses and facilities, trolleybuses, monorails, heavy (subway) and light rail, passenger rail (including both commuter rail and long distance rail), automated guide-way transit, inclined planes, and cable cars, designed to transport customers on regional and local routes.
Pipelines	Includes vast networks of pipeline that traverse hundreds of thousands of miles throughout the country, pipeline city gate stations, distribution networks and terminals that transport and distribute nearly all of the Nation's natural gas and 65 percent of hazardous liquids, as well as various chemicals. These pipeline networks are operated by over 3,000 operators.

Table 8. Transportation Systems Sector Modal Divisions[174]

The transportation sector relies in the annual federal data call to develop a list of assets, systems, and networks that make up transportation CIKR. The sector utilizes consequence to which assets, systems, and networks are most critical, based on "hazard-specific" scenarios.[175] According to the sector plan, transportation CIKR is prioritized

[174] Ibid. 15–16.

[175] Ibid., 4.

using four primary parameters: intelligence and risk assessments; legislative and executive requirements; budget and implementation constraints; and safety and privacy considerations and stakeholder concerns.[176]

The *Transportation Sector Plan* states, "State and local governments are responsible to manage sector protection within their jurisdictions." Furthermore, it states, "local governments represent the "front lines" for first responses to incidents involving sector assets." Lastly, in order to meet sector resiliency goals, state and local governments must assist in collecting infrastructure information.[177] This places a large amount of responsibility on state and local partners in order to meet sector protection and resiliency.

15. Water and Wastewater Systems Sector

The water and wastewater sector has two key subsectors: water treatment, storage, and distribution and wastewater treatment. The water subsector includes: drinking water and water to meet healthcare, fire protection, and heating and cooling processes. The sector plan states that "there are approximately 153,000 Public Water Systems of various sizes and users in the United States." The physical elements of a drinking water system include: water source; conveyance; raw storage; treatment; treated water storage; distribution system; and a monitoring system (Figure 5).[178]

[176] Ibid., 40–41.

[177] Ibid., 22.

[178] U.S. Department of Homeland Security, *Water and Wastewater Systems Sector-Specific Plan*, 2010, U.S. Department of Homeland Security, http://www.dhs.gov/xlibrary/assets/nipp-ssp-water-2010.pdf, 8–9.

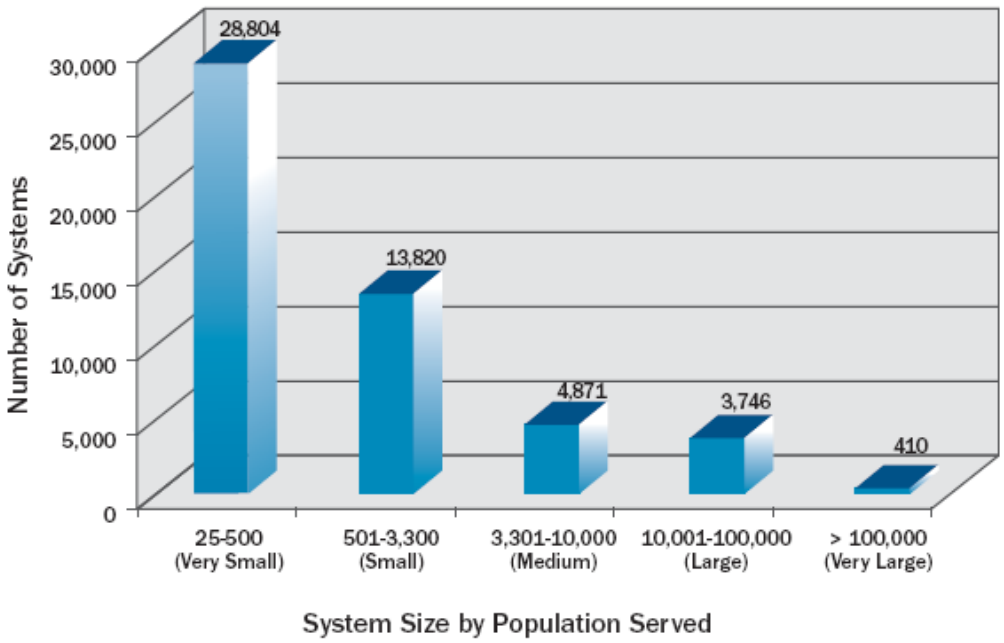

Figure 5. Number of Community Systems and System Size[179]

There are over 16,500 wastewater treatment systems in the U.S. that provide treatment of domestic sewage to over 227 million people (see Figure 6).[180] Additionally, many systems provide treatment of waste water from industrial facilities. Failure or disruption of these systems can result in loss of life or significant public health and environmental impacts. Wastewater systems include the following physical elements: collection system; raw influent storage; treatment system; treated water storage; effluent/discharge; and monitoring system.[181]

[179] Ibid., 8.

[180] Ibid., 11.

[181] Ibid.

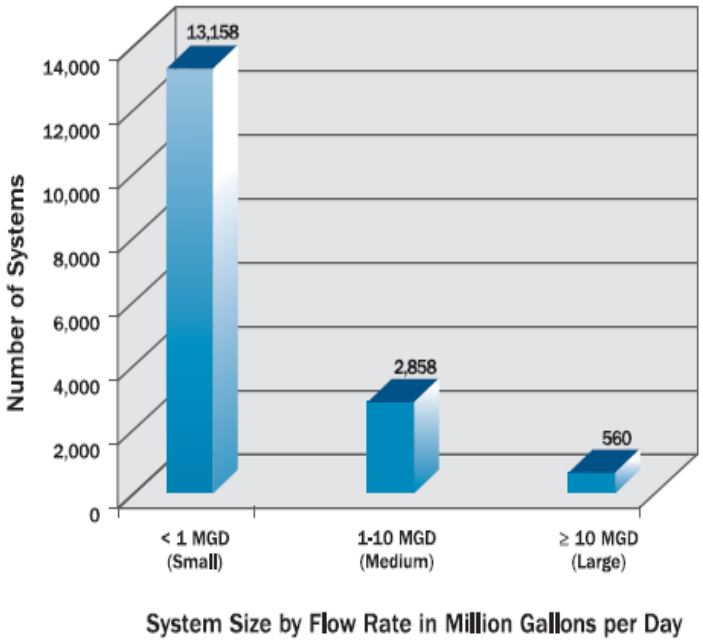

Figure 6. Numbers of Publicly Owned Treatment Systems and System Size[182]

While the sector-specific plan identifies wastewater as a subsector much of the plan is dedicated to identifying and assessing the water subsector.[183] The water subsector has developed its own criteria for identifying CIKR assets, systems, and networks. This model includes four criteria used for assessing CIKR priority Levels: population served; quantity of chlorine gas stored on-site; economic impact; and critical customers served.[184] Table 9 highlights the criteria utilized in the water sector. This model is scalable for use by state and local planning partners.

[182] Ibid., 10.

[183] Ibid.

[184] Ibid., 30.

Level Criteria	Level 1	Level 2	Level 3	Level 4
Drinking Water and Wastewater - Population Served **(Drinking water only: retail plus wholesale)**	≥ 1million	25,000 – 1 million	3,300 – 25,000	< 3,300
On-site Gaseous Chlorine Storage (average daily volume stored)	≥ 40 tons	20 – 40 tons	1 – 20 ton(s)	< 1 ton
Economic Impact **(regional impact; not including value of statistical life)**	≥ $100 billion	$5 – $100 billion	$100 million—$5 billion	< $100 million
Critical Customers Served	*Federal Government Defined*	*Federal Government Defined*	*Two or more of the following:* • Level 1 Trauma • Venue that holds 10,000 or more people • National Icons • Key Defense facilities • Key Defense Industrial Base assets	Not Applicable

Table 9. Water Sector Level Criteria[185]

[185] Ibid.

The *Water Sector Plan* indicates the role of State and local jurisdictions as supporting the sector's planning, protection, and resiliency initiatives.[186] Among the sector goals and objectives related to state and local jurisdictions are:

- Goal 4: Increase communication, outreach and public confidence;
- Objective 2: Enhance communication and coordination among utilities and federal, state, and local officials and agencies to provide information about threats.[187]

F. KEY FINDINGS OF SECTOR-SPECIFIC PLANS

Each sector-specific plan identifies some methodology and has established an all-hazards approach for identifying assets, systems, and networks within their respective sector. However, the criteria utilized varies widely from clear, concise, consequence based, as in the water sector, to the reliance on owners and operators of CIKR or subject matter experts. There is no evidence that the sector plans are scalable for use at the state and local jurisdictional Level. This is supported in an October 2011 State, Local, Tribal, and Territorial Government Coordinating Council report on *Northeast Critical Infrastructure Protection Programs*. Among the major findings in the report were that:

> …the large majority of State CIP coordinators indicated a need for clearer guidance from U.S. Department of Homeland Security National Protection and Programs Directorate Office of Infrastructure Protection (NPPD/IP) about what constitutes a "critical" asset. Respondents reported that NPPD/IP has been reluctant to produce criteria apart from the guidance included in NCIPP.[188]

The report also found that the northeast states have focused their CIKR programs on assessing "core lifeline sectors- water and waste water, energy, communications, transportation, and information systems."[189]

---

[186] Ibid., 1.

[187] Ibid., 17.

[188] State, Local, Tribal, and Territorial Government Coordinating Council, *Final Report: Northeast Critical Infrastructure Protection Programs* (Washington, DC: State, Local, Tribal, and Territorial Government Coordinating Council, 2011), 6.

[189] Ibid., 8.

Most sectors reference the annual federal data call or the National Critical Infrastructure Prioritization Program (NCIPP) as the established parameters for states to report on Level 1 and Level 2 CIKR. The NCIPP utilizes a consequence based criteria for identifying Level 1 and Level 2 assets.[190] However, the success of the NCIPP relies on voluntary participation from public and private CIKR partners for populating the NCIPP asset list.[191] Among the finding in GAO-13-296 relating to state participation on the NCIPP program was that "most state officials contacted reported that it is difficult to nominate assets to the NCIPP list using the consequence-based criteria, and two officials said that they are considering whether to continue to participate in the NCIPP process."[192] Furthermore, "Homeland security officials representing 13 of the 15 states told us that they believe that the nomination process is moderately difficult or very difficult and at least two states no longer participate due to the time and effort required."[193]

Numerous references in each sector plan are made to the importance of engaging or collaborating with local jurisdictions in CIKR planning, but there is no information within each sector plan to assist local identification of assets, systems and networks. Many sectors identify the SLTTGCC as the link between the federal sector-specific agencies (SSA) and state and local jurisdictions. The State, Local, Tribal, and Territorial Government Coordinating Council report on *Northeast Critical Infrastructure Protection Programs* cites several potential disconnects with the relationship between the federal SSA's and state and local participation in CIKR planning. For example, the reports states:

> The NPPD/IP develops and deploys programs to the field under the assumption that each State has a robust and dedicated CIP program office. In reality, these small State CIP units are doing much with little, but they need NPPD/IP to design programs with their staff resources and associated capabilities in mind.[194]

---

[190] Government Accountability Office, *Critical Infrastructure Protection*, 13.

[191] Ibid., 9

[192] Ibid., 30.

[193] Ibid.

[194] State, Local, Tribal, and Territorial Government Coordinating Council, *Final Report*, 5.

Furthermore it notes, "States have found it difficult to interest local government in sustained and systematic CIP efforts, except in situations where federal funding streams are attached."[195] Lastly, related to local participation the report explains:

> …local government officials interviewed by the Council indicated that their primary activities focus on identifying assets and conducting or participating in a limited number of site assessments. The primary obstacle to extending CIP to the local Level is time and resources.[196]

[195] Ibid.

[196] Ibid., 6.

THIS PAGE INTENTIONALLY LEFT BLANK

V. STATE OF NEW HAMPSHIRE CRITICAL INFRASTRUCTURE PROTECTION

A. PROBLEM

The earliest references to formal critical infrastructure protection (CIP) at the federal Level can be found in *Presidential Decision Directive 63* (PDD-63) issues in 1998 by President William J. Clinton. PPD-63 states, "It has long been the policy of the United States to assure the continuity and viability of Critical Infrastructures." [197]

PPD-63 states a national goal as:

> No later than the year 2000, the United States shall have achieved an initial operating capability and no later than five years from today (May 22, 1998) the United States shall have achieved and shall maintain the ability to protect the nation's Critical Infrastructures from intentional acts.[198]

The guidelines for implementing this directive specifically reference state and local governments as follows: "close cooperation with state and local governments and first responders is essential for a robust and flexible infrastructure protection program. All critical infrastructure plans and action shall take into consideration the needs, activities and responsibilities of state and local governments and first responders."[199]

Research conducted of existing state homeland security strategies shows that the state of New Hampshire is the only state that has worked to develop a "state-specific" criteria for identifying CIKR. Prior to the terrorist attacks of September 11, 2001 the state of New Hampshire had little to no process in place to identify and evaluate the risks to infrastructure assets that are critical to state and/or local jurisdictions.

---

[197] White House, *Presidential Decision Directive/NSC 63*.

[198] Ibid., 2.

[199] Ibid., 4.

B. SOLUTION

1. State of New Hampshire Critical Infrastructure Protection Program

The importance of developing a CI asset list and begin protection planning at other than the federal Level was identified post September 11, 2001. Representatives of several state agencies, led by the state of New Hampshire National Guard, were tasked by then Governor Jeanne Shaheen with developing a list of assets that were critical within the state of New Hampshire. This processed has evolved over the last 12 years with three distinct efforts to identify assets that are critical to the State of New Hampshire.

2. Version 1

Representatives of the National Guard were tasked with developing a list of critical infrastructure assets and developing a methodology for assessing each assets criticality. This process identified 11 critical infrastructure sectors are shown in Table 10.[200]

1. Agriculture and Food	• The supply chains for feed, animals, and animal products. • Crop production and the supply chains of seed, fertilizer, and other necessary related materials; and • The post-harvesting components of the food supply chain, from processing, production, and packaging through storage and distribution to retail sales, institutional food services and restaurant or home consumption.
2. Water	• Fresh water supply • Wastewater collection and treatment
3. Public Health	• State and local health departments • Hospitals • Health clinics • Mental health facilities • Nursing homes • Blood-supply facilities • Laboratories • Mortuaries • Pharmaceutical stockpiles
4. Emergency Services	• Fire • Rescue • Emergency Medical Service

[200] Thomas Haydon, *State of New Hampshire Critical Infrastructure Categories*, (internal document New Hampshire Advisory Council on Emergency Preparedness and Security, State of New Hampshire, Department of Safety, 2004).

	• Law Enforcement
5. Defense Industrial Base	• Department of Defense installations and the private defense industry
6. Telecommunications	• Voice and data services • Public Switched Telecommunications Network (PSTN) • Internet • Physical facilities • Switches, cables, other equipment • Cellular, microwave, and satellite services.
7. Energy	• Electricity (Generation, transmission and distribution, and control and communications) • Oil and Gas o Oil - Oil production, crude oil transport, refining, product transport and distribution, and control and other external support systems. o Gas—Exploration and production, transmission, and local distribution.
8. Transportation	• Aviation • Maritime traffic • Rail • Pipelines • Highways • Trucking and bussing • Public mass transit
9. Banking and Finance	No specific asset references
10. Chemical Industry and Hazardous Materials	No specific asset references
11. Postal and Shipping	No specific asset references

Table 10. State of New Hampshire CI Sectors[201]

The following methodology was presented as a mechanism to prioritize the assets identified in the above sectors (Table 11).[202] However, evidence in the literature

[201] Ibid.

[202] Ibid.

reviewed and a follow-up interview with the former State Director of Homeland Security suggests that this process was only utilized to evaluate select assets.[203]

1. Impact on critical category:

Red	Catastrophic—complete loss of output, production or service
Orange	Significant—66% or more loss output, production or service
Yellow	Serious—33% or more loss output, production or service
Blue	Degraded—10% - 33% loss of output, production or service
Green	No significant effect

2. Recoverability:

Red	Replacement or repair requires 1 month or longer
Orange	Replacement or repair requires 1 week to 1 month
Yellow	Replacement or repair requires 3 days to 1 week
Blue	Replacement or repair requires 1 to 3 days
Green	Same day replacement or repair

3. Likelihood of being attacked:

Red	Most likely imminent
Orange	Highly likely
Yellow	Probable
Blue	Possible
Green	Not likely

4. Threat to life/safety:

Red	250+ injured or killed
Orange	101—250 injured or killed
Yellow	26—100 injured or killed
Blue	6—25 injured or killed
Green	1—5 injured or killed

Table 11. State of New Hampshire CI Assessment Criteria[204]

[203] Christopher Pope (former State of New Hampshire Homeland Security Director), interview with the author, August 19, 2013.

[204] Ibid.

3. Version 2

The second iteration began with the formal creation of the Director of Homeland Security and Emergency Management position within the state Department of Safety in July 2006 and the implementation of the 2005 state of *New Hampshire Homeland Security Strategy*.[205] This strategy included one goal and four objectives related to CIKR protection as follows:[206]

- Goal: Protection—To achieve and sustain capabilities that enable the state of New Hampshire to reduce the vulnerability of critical infrastructure or key resources (CIKR) in order to deter, mitigate, or neutralize catastrophic events including terrorist attacks, major disasters, and other emergencies.
- Objective 1: Continue to develop/update a list of critical infrastructure and key assets in the state of New Hampshire;
- Objective 2: Develop/update a plan to reduce vulnerabilities of critical infrastructure and key assets in the state of New Hampshire with all participating jurisdictions;
- Objective 3: Assess and determine equipment necessary to improve security in and around key infrastructure in the state of New Hampshire;
- Objective 4: Develop exercises or incorporate into planned exercises for protection of critical infrastructure in the state of New Hampshire.

A March 2008 *NH Department of Emergency Services Critical Infrastructure and Key Resources (CI/KR) Preparedness Report* identified over 3,000 assets that are critical to the state. This list was developed by interviewing 10 county sheriffs and utilizing the fiscal years 2007 and 2008 critical infrastructure identification criteria. The primary goal was to identify assets that meet the federal criteria, and it but also identified infrastructure important to the state of NH that did not meet the federal criteria.[207] This list was inclusive of both hard targets, including critical transportation infrastructure, water treatment and storage facilities, fuel storage facilities, as well as "soft targets," such as schools and shopping malls.

---

[205] State of New Hampshire, "Revised Statutes Annotated," 2006, State of New Hampshire, http://www.gencourt.state.nh.us/rsa/html/i/21-p/21-p-mrg.htm.

[206] State of New Hampshire Homeland Security Strategy, 2005 (restricted-access document).

[207] State of New Hampshire, Department of Safety, *State of New Hampshire Homeland Security CI/KR Identification Report* (restricted-access document).

4. Version 3

The current program began in 2008 as a result of the state of *NH Preparedness Report* and release of the *Interim National Infrastructure Protection Plan*. This reports states that the state will adopt the following mission related to CIKR protection:

> To achieve and sustain capabilities that enable the State of New Hampshire to reduce the vulnerability of critical infrastructure or key resources in order to deter, mitigate, or neutralize catastrophic events including terrorist attacks, major disasters, and other emergencies.[208]

The report further listed a major goal of developing a "state-Level" criteria for determining critical infrastructure with an objective of making the original list more manageable.[209] To meet this goal a critical infrastructure protection (CIP) subcommittee of the Governor's Advisory Council on Emergency Preparedness and Security (ACEPS) was created in June, 2008.

The CIP subcommittee was given two goals:

1. **Identify an assessment tool that NH can use to define state critical infrastructure and**
2. **Identify criteria for defining state critical infrastructure**

The committee chose the following methodology for assessing critical infrastructure:

- Utilize the 17 critical infrastructure sectors as defined in the Interim National Infrastructure Protection Program (NIPP)[210] (later this was expanded to the 18 sectors as identifies in the 2009 NIPP);[211]
- Add a "special events" sector for New Hampshire;
- Assign a lead person to work on each sector;
- Review one sector per month;
- Review interdependencies between sectors;

---

[208] State of New Hampshire, Department of Safety, *State of New Hampshire Preparedness Report*, (Concord, NH: State of New Hampshire, Department of Safety, 2008), (restricted-access document).

[209] Ibid.

[210] U.S. Department of Homeland Security, *Interim National Infrastructure Protection*.

[211] U.S. Department of Homeland Security, *National Infrastructure Protection Plan*.

- Use the federal fiscal year 2009 data call as a base guideline for CI/KR asset definitions and;
- Develop an asset criterion that is quantitative and as narrow as possible.[212]

As a result of the CIP committee's work over the last three years, each of the definitions have been developed for each of the federal sectors resulting in the identification of approximately 340 critical infrastructure assets in the state of New Hampshire. One addition to the state of New Hampshire program was the creation an independent "special events" sector. A follow-up committee's leadership met with the Department of Homeland Security Special Events Office and found that it was just a collection agency for events deemed "special" by a state or organization and lacked a criteria for strictly defining special events. In addition, the NH program uses DHS data gathering tools to develop the state criteria, but it has not adequately defined the implications for having events on the State list. The current list is utilized by both the United States Department of Homeland Security Infrastructure Protection Protective Security Advisor and the State of New Hampshire Information and Analysis Center to perform security assessments of CI/KR assets throughout the state.

Beginning in September of 2007, the State Homeland Security Grant Program began allocating a portion of the required 80 percent local share towards critical infrastructure protection as follows (see Table 12):[213]

[212] State of New Hampshire ACEPS CIP Subcommittee, "Meeting Minutes," Concord, NH, June 8, 2008.

[213] State of New Hampshire Department of Safety, "Grants Management," accessed August 15, 2013, https://www.nh.gov/safety/divisions/homeland/2012/index.htm.

Year	80% Local Share	CIP Allocation
2007	$3,056,000	$350,000
2008	$3,702,000	$500,000
2009	$3,914,700	$500,000
2010	$3,813,978	$500,000
2011	$2,718,292	$250,000
2012	$2,241,052	$150,000
Totals	**$19,446,022.00**	**$2,250,000.00**

Table 12. State of New Hampshire CI Protection Spending 2007–2012[214]

There are two primary conditions that determine CIP grant eligibility for local jurisdictions: 1) assets must be identified on the state critical infrastructure list and 2) identified assets must have vulnerability assessment completed by either the state of NH or the Department of Homeland Security.[215]

C. ANALYSIS

The state of New Hampshire is the only state to date that has worked to develop "state-specific" criteria for identifying CIKR. The New Hampshire program follows the federal strategy by assigning sector-specific agencies, but it limits the possibility of "stove-piping" by having all sector subject matter experts report back to a main Critical Infrastructure Committee. The Critical Infrastructure Committee then makes a recommendation to the State of New Hampshire Governor's Advisory Council on Emergency Preparedness and Security for adoption. The state of New Hampshire program was developed definitions for identifying CIKR assets that are critical to the state or region.[216] This strategy can assist the state in developing CI protection plans and justifying the allocation of State Homeland Security Grant monies for buying down risk. There is little evidence in this program to indicate the engagement of local jurisdictions in

[214] State of New Hampshire Department of Safety, Grants Management Unit, request for information related to homeland security grant funding, August 12, 2013, via email correspondence.

[215] Ibid.

[216] State of New Hampshire, Department of Safety, *State of New Hampshire Homeland Security CI/KR Identification Report* (restricted-access document).

the development of Critical Infrastructure Protection Programs. As an example, as of August 2013, of the $2,250,000 allocated for CIKR protection only $810,809 have been awarded to local jurisdictions for CIKR projects. This does not include pending grant proposals for award under the 2011 and 2012 funding.[217] Furthermore, while the committee set a goal to use a qualitative approach to developing asset definitions and lists, a review of committee minutes and asset list suggests that in at least one sector, agriculture and food, the asset list was largely developed in a subjective manner and remains incomplete as of August 2013.

D. CONCLUSION

The State of New Hampshire CI/KR Protection Program lays the foundation for identifying assets that are critical to the state and region. The program was able to meet the 2008 state preparedness goal of developing a "state-Level" criteria for determining critical infrastructure with an objective of making the original list more manageable. While the program has begun to assess CI/KR assets throughout the state, the program still needs to better engage local jurisdictions in CI/KR protection and resiliency planning.

[217] State of New Hampshire Department of Safety, Grants Management Unit, request for information related to homeland security grant funding, August 12, 2013, via email correspondence.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSION AND RECOMMENDATIONS

"Alone we can do so little; together we can do so much"

Helen Keller[218]

A. CONCLUSION

This research sought to examine the relationship between the National Infrastructure Protection Program and local critical infrastructure planning. Specifically, it looked at to what extent does the federal criteria for identifying federal critical infrastructure and key resources apply to state and local identification of critical infrastructure and key resources. As the first line of defense and response to incidents within their jurisdictions, local officials must work to identify what critical infrastructure exists within and more importantly, if lost, what will have an impact on the community's ability to provide services.

While some states have worked to develop CIKR plans and do participate in the annual federal data call or the National Critical Infrastructure Prioritization Program, it is unclear on the extent of participation or the number of assets reported. Conversely, all 50 states and approximately 70 percent of the communities in the U.S. have approved hazard mitigation plans under FEMA's Pre-Disaster Mitigation Program since its inception.[219] Between 2007 and 2012, FEMA awarded 1.7 billion dollars in hazard mitigation planning grants.[220] During a similar period, FEMA spent over 17.3 billion dollars on disaster relief.[221] This data suggests that the U.S. is not committing sufficient resources towards

---

[218] Helen Keller International, "Helen Keller's Legacy," Helen Keller International, http://www.hki.org/about-helen-keller/helen-kellers-legacy/.

[219] Office of the Inspector General, U.S. Department of Homeland Security, *Survey of Hazard Mitigation Planning*, 2012, Office of the Inspector General, http://www.oig.dhs.gov/assets/Mgmt/2012/OIG_12-109_Aug12.pdf, 1.

[220] Ibid.

[221] Office of Budget and Management, *OMB Report on Disaster Relief Funding to the Committees on Appropriations and the Budget of the U.S. House of Representatives and the Senate*, 2011. White House, http://www.whitehouse.gov/sites/default/files/omb/assets/legislative_reports/disaster_relief_report_sept2011.pdf.

prevention and mitigation of the impacts associated with natural and manmade disasters and that inaction related to CI protection and, more importantly, resiliency planning is more costly.

The analysis of the NIPP and subsequent sector-specific plans indicates that there is no clear connection between the NIPP and local government CIKR protection and resiliency planning. Specifically, the federal criteria for identifying assets, systems, and networks is too broad in scope and provides little direction for identifying CIKR assets, systems, and networks at not only the federal and state Level, but also for local jurisdictions. It also found that despite clear references to engaging state and local jurisdictions in planning, there was no evidence to support collaboration efforts between federal, state, and local jurisdictions. This is contrary to the *National Security Strategy*, which states, "Collaboration across the government—and with our partners at the state, local, and tribal Levels of government, in industry, and abroad—must guide our actions."[222]

The terrorist attacks of September 11, 2001, Hurricane Katrina in 2005, "Super Storm" Sandy in 2012, and the recent widespread flooding in Colorado only reinforce the need for collaboration between federal, state, and local government for pre-event planning, preparation, response, and recovery. Connecting the different planning processes and enhancing information sharing will make the U.S. one step closer to closing planning silos.

B. RECOMMENDATIONS

The following recommendations are proposed to help align federal, state, and local critical infrastructure planning. Each recommendation proposes to identify the implications of just doing business as usual with current critical infrastructure protection and resiliency programs. The author suggests that this strategy will increase participation in critical infrastructure protection and resiliency planning by providing clear, scalable guidance for local jurisdictions without creating new planning processes.

[222] White House, *National Strategy for Information Sharing and Safeguarding*, 2012, White House, http://www.whitehouse.gov/sites/default/files/docs/2012sharingstrategy_1.pdf, 14.

1. Strengthen the Relationship among Federal, State, and Local CIKR Planning

The current federal approach to CIKR planning utilizes a "top down" methodology where sector-specific agencies define the parameters for their respective sector and "voluntarily" request asset, systems, and networks lists from states. Strengthening participation by both state and local jurisdictions will ensure that no CIKR assets, systems, and networks and key interdependencies overlooked. The second barrier that needs to be addressed is information sharing. There are two suggested components to establishing this link.

a. Component 1

Redefine the CIKR reporting process from a "top down" to an "up and down" information flow. This can help to develop necessary relationships and built on trust and credible information. Locals would submit CIKR lists to the state, the state would compare this list with state criteria and ultimately report Level 1 and Level 2 CIKR to federal CIKR sector-specific agencies. Conversely, the federal sectors would share information to states and states to appropriate local jurisdictions related to critical assets, systems, and networks (see Figure 7). One potential barrier to the latter is the lack of a consistent security classification for information related to CIKR assets, systems, or networks.

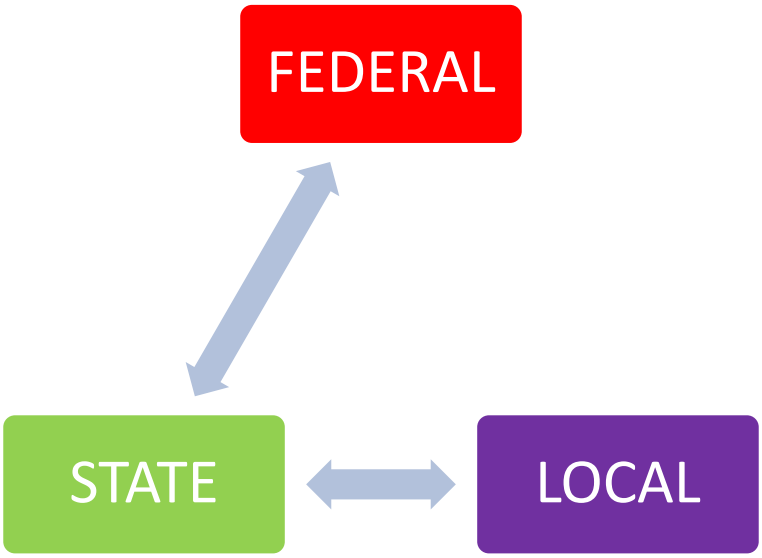

Figure 7. CIKR Information-Sharing Relationship

b. Component 2

Implement the goals and objectives related to information sharing at the State and local Levels as identified in the *National Strategy for Information Sharing and Safeguarding*. Specifically, core principal 3—"Information Informs Decision Making," which states, "National security depends on easy access to information at the Federal, state, and local Level."[223] In the context of critical infrastructure, this can be accomplished by conducting outreach and training to local officials on the Protected Critical Infrastructure Information (PCII) Program. This will provide local officials the necessary link for sharing information between private owners of CIKR and state CIKR program officials.

2. Link Hazard Mitigation with National Infrastructure Protection and Resiliency Planning

The process for developing hazard mitigation plans utilizes a similar methodology as the *National Infrastructure Protection Plan*. Each plan focuses on a risk assessment strategy for assessing and identifying critical assets, networks, and systems. As noted above, approximately 70 percent of U.S. communities and all 50 states are submitting

[223] Ibid., 7.

hazard mitigation plans. This recommendation suggests the development of a "hybrid" planning process incorporating key elements of hazard mitigation planning and the NIPP. This example of integration is supported in the 2009 version of FEMA's *Comprehensive Preparedness Guide*, which suggests that aligning of planning efforts, such as critical infrastructure identification, prioritization, and protection, national preparedness and planning, and continuity of operations, combined with the national incident management system, national response framework, and the national preparedness guidelines, determines how federal, state, and local agencies work to prevent, prepare, respond to and recover from natural and manmade disasters.[224]

The benefits of this approach will be (1) greater participation by locals in identifying critical assets, systems, and networks and (2) less reliance on additional resources for completion. One key finding on the SLTTGCC *Northeast Critical Infrastructure Protection Programs* report was the lack of time and resources for CIKR planning.[225] One potential obstacle is a lack of funding at the local Level to facilitate planning activities. This may be overcome by increasing pre-disaster hazard mitigation grant funding opportunities for local jurisdictions or expanding the use of state homeland security grant funds for CIKR/mitigation planning (Figure 8).

[224] Federal Emergency Management Agency, *Developing and Maintaining State, Territorial, Tribal, and Local Government Emergency Plans: Comprehensive Preparedness Guide*, 2009, Readiness and Emergency Management for Schools, http://rems.ed.gov/docs/FEMA_GovernmentEmergencyPlans.pdf, 4–2.

[225] State, Local, Tribal, and Territorial Government Coordinating Council, *Final Report*.

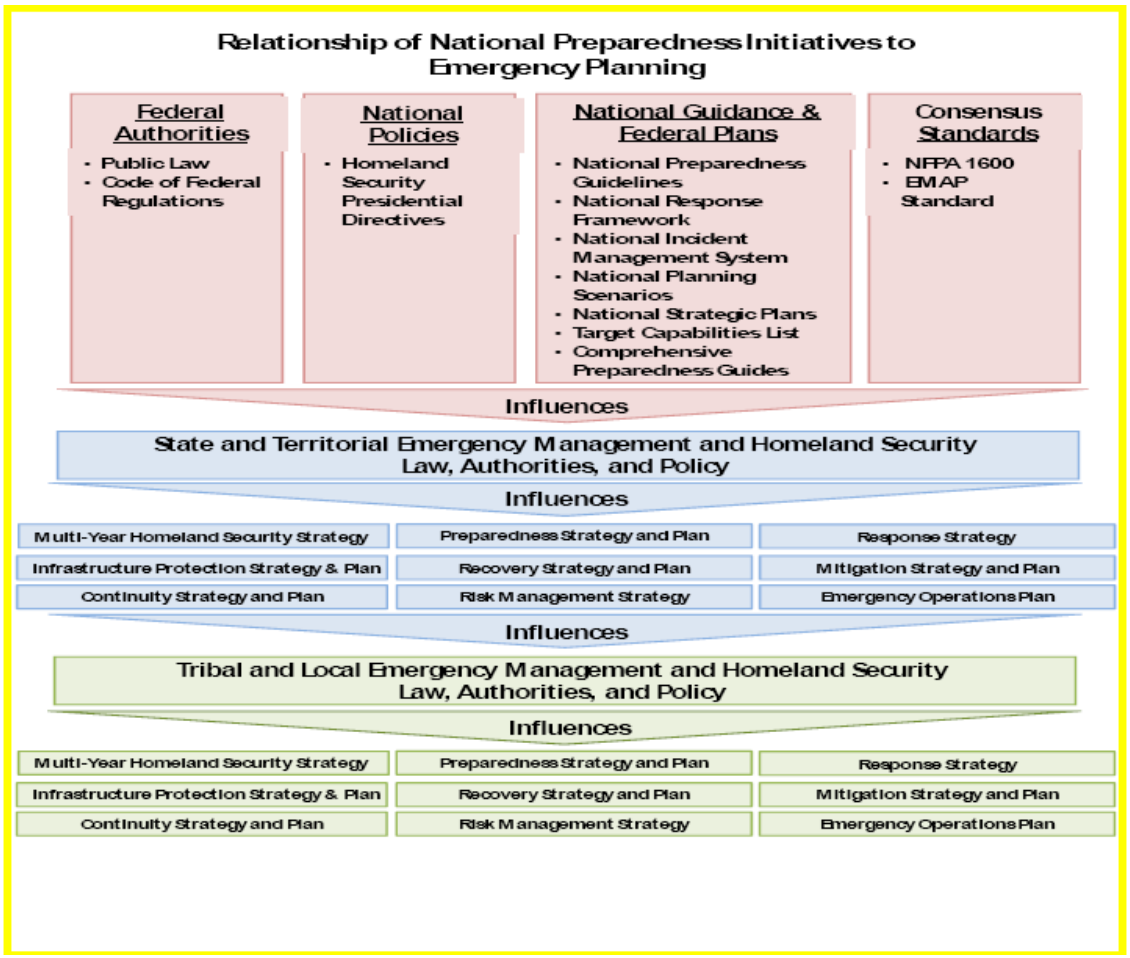

Figure 8. Relationships of the National Preparedness Initiatives to Emergency Planning[226]

3. Value Proposition

The proposed recommendation to develop standard CIKR asset definitions and intersecting the planning components of the NIPP and hazard mitigation planning for CIKR asset identification should be considered. The merits of this effort and possible outcomes will be development of a CIKR flow model that interconnects federal, state and local definitions. This information would allow local governments to develop CIKR protection strategies, develop resiliency plans, better mitigate natural and manmade disasters and develop partnerships with the private sector. With tight municipal budgets and a multitude of obligations competing for local official's time, clear definitions are

[226] Ibid, 4–3.

necessary to build effective local CIKR protection and resiliency programs. Lastly, shifting the local focus on pre-disaster mitigation and resiliency planning and an increase in pre-disaster grant funding may have a positive impact by reducing the reliance on federal disaster relief funds. The following figure highlights the use of the "eliminate-reduce-raise-create" grid from *Blue Ocean Strategies* to suggest the necessary changes to the federal approach to critical infrastructure protection programs that will allow for better alignment with state and local partners.

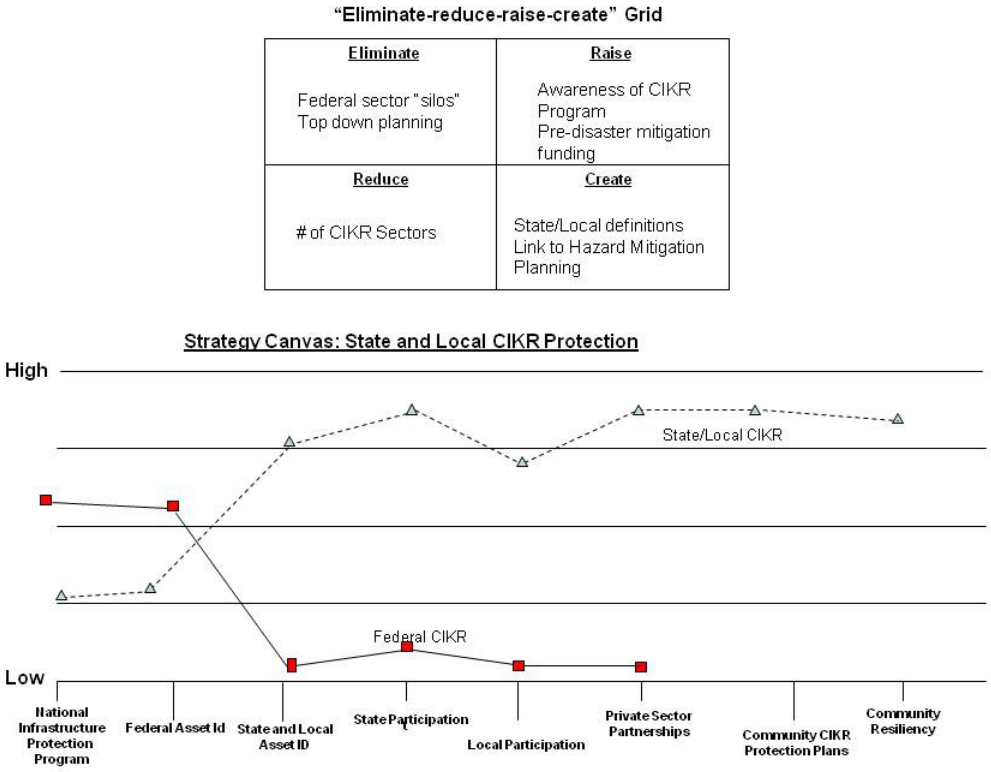

Figure 9. Strategy Canvas[227]

[227] W. Chan Kim and Renée Mauborgne, *Blue Ocean Strategy: How to Create Uncontested Market Space and Make the Competition Irrelevant* (Boston, MA: Harvard Business School Press, 2005).

4. Create Standard Asset Definitions for All CIKR Sectors

The missing links in each of the above planning process are standard definitions for critical asset, system, and network identification. Creating a standard, scalable consequence based criteria will provide clear guidance for developing CIKR lists at the federal, state, and local Levels. Use of a consequence based criteria based on the four consequences outline in the NIPP: "public health and safety (i.e., loss of life and illness); economic (direct and indirect); psychological; and governance or mission impacts." [228] Consequence definitions will allow planner at all Levels to assess assets, systems, and networks in a uniform manner and in most cases are easier to identify. The scope of the definition should also be expanded to include critical nodes. Critical nodes are defined as the most critical components of critical infrastructure.[229] The use of the other elements in the risk equation, threat, and vulnerability cannot be overlooked. Although threats and vulnerabilities can vary widely between federal, state, and local jurisdiction, guidance for determining threat and vulnerabilities should be developed in concert with state and local jurisdictions.

[228] U.S. Department of Homeland Security, *National Infrastructure Protection Plan*, 32.

[229] Lewis, *Critical Infrastructure Protection*, vii.

LIST OF REFERENCES

Commonwealth of Massachusetts, Executive Office of Public Safety and Security. *Commonwealth of Massachusetts Homeland Security Strategy*. 2007. http://www.mass.gov/eopss/docs/helpus-helpyou/state-homeland-security-strategy-092307.pdf.

Council of State Governments. "State Officials Guide to Critical Infrastructure." 2003. Council of State Governments. http://www.csg.org/knowledgecenter/docs/SOG03CriticalInfrastructure.pdf.

Federal Emergency Management Agency. "Disaster Declarations." Federal Emergency Management Agency. Accessed August14, 2013. http://www.fema.gov/disasters/grid/year.

———. "Hazard Mitigation Planning." Federal Emergency Management Agency. Accessed September 14, 2013. http://www.fema.gov/multi-hazard-mitigation-planning.

———. *State and Local Hazard Mitigation Planning—How-to Guide*. 2001. Federal Emergency Management Agency. http://www.fema.gov/library/viewRecord.do?id=1880.

General Accounting Office. *Critical Infrastructure Protection* (GAO-01-323). 2001. Homeland Security Digital Library. https://www.hsdl.org/?view&did=197.

Government Accountability Office. *Critical Infrastructure Protection: DHS List of Priority Assets Needs to Be Validated and Reported to Congress* (GA0-13-296). 2013. Government Accountability Office. http://www.gao.gov/assets/660/653300.pdf.

Federal Emergency Management Agency. *Developing and Maintaining State, Territorial, Tribal, and Local Government Emergency Plans: Comprehensive Preparedness Guide*. 2009. Readiness and Emergency Management for Schools. http://rems.ed.gov/docs/FEMA_GovernmentEmergencyPlans.pdf.

Haydon, Thomas. *State of New Hampshire Critical Infrastructure Categories*. Internal document New Hampshire Advisory Council on Emergency Preparedness and Security, State of New Hampshire, Department of Safety, 2004.

Helen Keller International. "Helen Keller's Legacy." Helen Keller International. http://www.hki.org/about-helen-keller/helen-kellers-legacy/.

Hurricane Sandy Rebuilding Task Force. “Fact Sheet: Progress to Date.” August 19, 2013. U.S. Department of Housing and Urban Development. http://portal.hud.gov/hudportal/HUD?src=/press/press_releases_media_advisories/2013/HUDNo.13-125

Jones, E. V., V. J. Lyford, M. K. Qazi, N. J. Solan, Y. Y. Haimes, *Virginia’s Critical Infrastructure Protection Study*, 2003. http://ieeexplore.ieee.org/xpl/abstractAuthors.jsp?tp=&arnumber=1242416&url=http%3A%2F%2Fieeexplore.ieee.org%2Fiel5%2F8798%2F27841%2F01242416

Kansas Division of Emergency Management. “Kansas State Homeland Security Strategy Goals and Objectives.” 2009. http://www.accesskansas.org/kdem/EMSWeb/pdf/library/State%20Strategy%20Fall%202009%20FINAL_1.pdf.

Kim, W. Chan and Renée Mauborgne. *Blue Ocean Strategy: How to Create Uncontested Market Space and Make the Competition Irrelevant*. Boston, MA: Harvard Business School Press, 2005.

Lewis, Ted G. *Critical Infrastructure Protection in Homeland Security*. Hoboken, NJ: John Wiley & Sons, Inc., 2006.

——— and Rudy Darken. “Potholes and Detours in the Road to Critical Infrastructure Protection Policy.” *Homeland Security Affairs*, 1, no. 2 (2005). http://www.hsaj.org/?article=1.2.1.

Miller, Robert. “Hurricane Katrina: Communications & Infrastructure Impacts.” In Threats at Our Threshold. 2012. http://astrumsat.com/wp-content/uploads/2012/04/KatrinaHurricaneComm.pdf.

Office of Budget and Management. *OMB Report on Disaster Relief Funding to the Committees on Appropriations and the Budget of the U.S. House of Representatives and the Senate*. 2011. White House. http://www.whitehouse.gov/sites/default/files/omb/assets/legislative_reports/disaster_relief_report_sept2011.pdf.

Office of the Inspector General, U.S. Department of Homeland Security. *Commonwealth of Pennsylvania’s Management of State Homeland Security Program and Urban Areas Security Initiative Grants*. 2011. Office of the Inspector General. http://www.oig.dhs.gov/assets/Mgmt/OIG_11-109_Sep11.pdf.

———. *State of Missouri’s Management of State Homeland Security Program and Urban Areas Security Initiative Grants Awarded during Fiscal Years 2005 through 2007*. 2010. Office of the Inspector General. http://www.oig.dhs.gov/assets/Mgmt/OIG_10-33_Jan10.pdf.

———. *Survey of Hazard Mitigation Planning*. 2012. Office of the Inspector General. http://www.oig.dhs.gov/assets/Mgmt/2012/OIG_12-109_Aug12.pdf.

O'Neil, D. J. "Statewide Critical Infrastructure Protection: New Mexico's Model." *TR News*, no. 211 (2000). http://onlinepubs.trb.org/onlinepubs/trnews/trnews211.pdf.

President's Commission on Critical Infrastructure Protection. "Critical Foundations—Protecting America's Infrastructure." 1997. Federation of American Scientists. http://www.fas.org/sgp/library/pccip.pdf.

State, Local, Tribal, and Territorial Government Coordinating Council. *Final Report: Northeast Critical Infrastructure Protection Programs*. Washington, DC: State, Local, Tribal, and Territorial Government Coordinating Council, 2011.

———. "SLTTGCC Fact Sheet." 2011. U.S. Department of Homeland Security. http://www.dhs.gov/xlibrary/assets/slttgcc-factsheet-508-2011-08-19.pdf.

State of New Hampshire ACEPS CIP Subcommittee. "Meeting Minutes." Concord, NH June 8, 2008.

State of New Hampshire. "Revised Statutes Annotated." 2006. State of New Hampshire. http://www.gencourt.state.nh.us/rsa/html/i/21-p/21-p-mrg.htm.

———, Department of Safety. "Grants Management." Accessed August 15, 2013. https://www.nh.gov/safety/divisions/homeland/2012/index.htm.

———. *State of New Hampshire Homeland Security CI/KR Identification Report*. March 10, 2008. (For official use only).

———. *State of New Hampshire Preparedness Report*. Concord, NH: State of New Hampshire, Department of Safety, 2008.

State of Vermont Division of Emergency Management and Homeland Security. *Vermont Homeland Security Strategy*. 2012. http://hsu.vermont.gov/sites/vhs/files/2013%20Vermont%20State%20Strategy%20FINAL%20101512.pdf.

———. *Vermont Infrastructure Protection Plan*. 2009. http://vem.vermont.gov/local_state_plans/eop.

U.S. Department of Homeland Security. *Banking and Finance Sector-Specific Plan*. 2010. U.S. Department of Homeland Security. https://www.dhs.gov/sites/default/files/publications/nipp-ssp-banking-and-finance-2010.pdf.

———. *Chemical Sector-Specific Plan*. 2010. U.S. Department of Homeland Security. http://www.dhs.gov/xlibrary/assets/nipp-ssp-chemical-2010.pdf.

———. *Commercial Facilities Sector-Specific Plan*. 2010. U.S. Department of Homeland Security. http://www.dhs.gov/xlibrary/assets/nipp-ssp-commercial-facilities-2010.pdf.

———. *Communications Sector-Specific Plan*. 2010. U.S. Department of Homeland Security. http://www.dhs.gov/xlibrary/assets/nipp-ssp-communications-2010.pdf.

———. *Critical Manufacturing Sector-Specific Plan*. 2010. U.S. Department of Homeland Security. http://www.dhs.gov/xlibrary/assets/nipp-ssp-critical-manufacturing-2010.pdf.

———. *Dams Sector-Specific Plan*. 2010. U.S. Department of Homeland Security. http://www.dhs.gov/xlibrary/assets/nipp-ssp-dams-2010.pdf.

———. *Defense Industrial Base Sector-Specific Plan*. 2010. U.S. Department of Homeland Security. http://www.dhs.gov/xlibrary/assets/nipp-ssp-defense-industrial-base-2010.pdf.

———. *Emergency Services Sector-Specific Plan*. 2010. U.S. Department of Homeland Security. http://www.dhs.gov/xlibrary/assets/nipp-ssp-emergency-services.pdf.

———. *Energy Sector-Specific Plan*. 2010. U.S. Department of Homeland Security. http://www.dhs.gov/xlibrary/assets/nipp-ssp-energy-2010.pdf.

———. *Food and Agriculture Sector Specific Plan*. 2010. U.S. Department of Homeland Security. http://www.dhs.gov/xlibrary/assets/nipp-ssp-food-ag-2010.pdf,

———. *A Guide to Critical Infrastructure and Key Resources Protection at the State, Regional, Local, Tribal and Territorial Level*. 2008. U.S. Department of Homeland Security. http://www.dhs.gov/xlibrary/assets/nipp_srtltt_guide.pdf.

———. *Health Care and Public Health Sector-Specific Plan*. 2010. U.S. Department of Homeland Security. http://www.dhs.gov/xlibrary/assets/nipp-ssp-healthcare-and-public-health-2010.pdf.

———. *Information Technology Sector-Specific Plan*. 2010. U.S. Department of Homeland Security. https://www.hsdl.org/?abstract&did=7899.

———. *Interim National Infrastructure Protection Plan*. 2005. Educase. http://net.educause.edu/ir/library/pdf/csd3754.pdf.

———. *National Infrastructure Protection Plan*. 2009. Department of Homeland Security. http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

———. *National Preparedness Goal*. 2011. Federal Emergency Management Agency. http://www.fema.gov/pdf/prepared/npg.pdf.

———. *Nuclear Reactors, Materials and Waste Sector-Specific Plan*. 2010. U.S. Department of Homeland Security. http://www.dhs.gov/xlibrary/assets/nipp-ssp-nuclear-2010.pdf.

———. *Transportation Systems Sector-Specific Plan*. 2010. U.S. Department of Homeland Security. http://www.dhs.gov/xlibrary/assets/nipp-ssp-transportation-systems-2010.pdf.

———. *Water and Wastewater Systems Sector-Specific Plan*. 2010. U.S. Department of Homeland Security. http://www.dhs.gov/xlibrary/assets/nipp-ssp-water-2010.pdf.

———, Office of the Inspector General. *Survey of Hazard Mitigation Planning*. 2012. http://www.oig.dhs.gov/assets/Mgmt/2012/OIG_12-109_Aug12.pdf.

U.S. Environmental Protection Agency. *Water Sector-Specific Plan*. 2010. U.S. Department of Homeland Security. http://www.dhs.gov/xlibrary/assets/nipp-ssp-water-2010.pdf.

Wales, Brandon. *2009 Tier I and II Data Call*. Washington, DC: U.S. Department of Homeland Security, 2009.

Whitaker, Eric "Preparing for a Disaster." Dictionary Quotes. July 2012. http://www.dictionary-quotes.com/emergency-preparedness-is-a-team-sport-eric-whitaker/.

White House. "The Federal Response to Hurricane Katrina: Lessons Learned." 2006. White House Archives. http://georgewbush-whitehouse.archives.gov/reports/katrina-lessons-learned/chapter5.html.

———. *National Strategy for Information Sharing and Safeguarding*. 2012. White House. http://www.whitehouse.gov/sites/default/files/docs/2012sharingstrategy_1.pdf.

———. *Presidential Decision Directive 7: Critical Infrastructure Identification, Prioritization, and Protection*. 2003. Department of Homeland Security. http://www.dhs.gov/homeland-security-presidential-directive-7.

———. *Presidential Policy Directive 21: Critical Infrastructure Security and* Resiliency. 2013. White House. http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California